Winter 2014

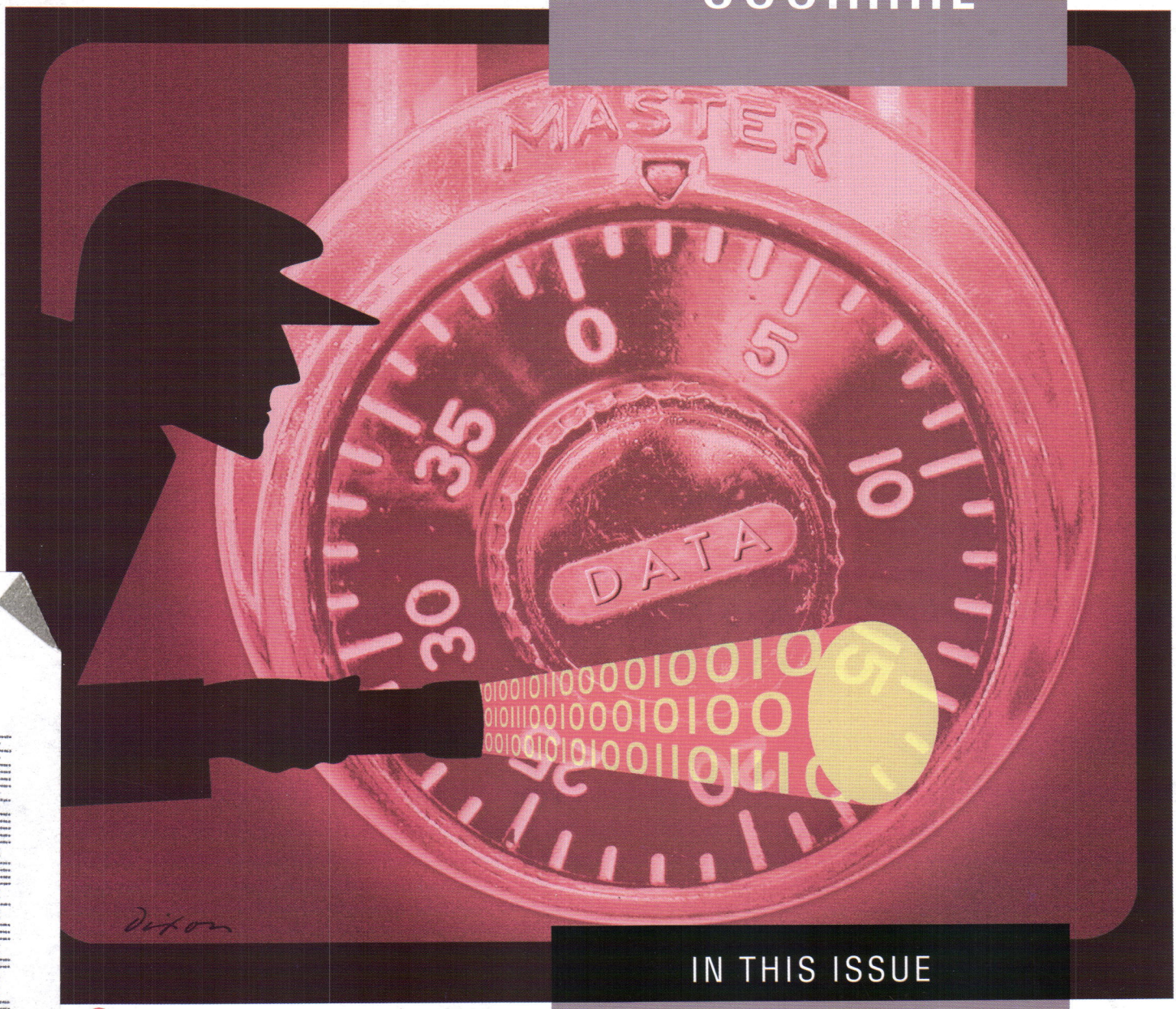
# ACUTA Journal of Telecommunications in Higher Education

2014/2015
Winter
Volume 18
Number 4

***Association for College and University Technology Advancement***

ACUTA

# JOURNAL




## IN THIS ISSUE

AVST | Unifying Communications®

# Meet TeamQ™

## The Next-Generation Informal Call Center for Higher Education

Welcome to TeamQ – the innovative informal call center solution from AVST that facilitates collaboration among workgroups. Your campus has many teams fielding calls, solving problems, juggling multiple service requests. These busy knowledge workers include the admissions office, IT help desk, financial aid office, counseling office, health services clinic, library – to name a few. TeamQ delivers high ROI by giving teams access to vital call center features at a fraction of the price of other solutions. Think UCD, ACD, agent desktop control with informative screen pops, supervisor interface, reports and much more.

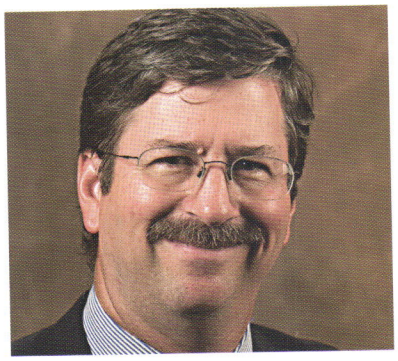
- Essential Call Center Features
- Affordable Price
- Goes Mobile – Delivers Calls to Smartphone, Tablets and Softphones
- Enables Agents to Multitask and Control Their Call Workflow
- Works with All Major PBXs
- Supports up to 250 Agents

**TEAMQ™**

Campus communications just got better.

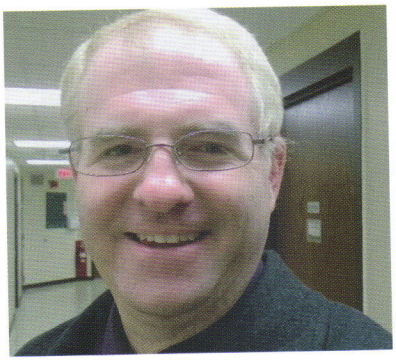
**avst.com/education**

## Quotes of Note



*Privacy is not about what you try to hide, but what you choose to reveal.*

**Matt Arthur, CISSP**
Director, Media Services and Incident Communications Solutions
Information Services and Technology
Washington University
St. Louis, MO



*In Information Assurance, the most powerful tool isn't hardware or software, but the ability to approach a new challenge pragmatically. The strongest mitigating controls are not built on selective interpretation and justification, but rather on our ability to be honest with ourselves about the reality of the issues before us.*

**Nicholas Davis**
Information Security Architect, IT
University of Wisconsin
Madison, WI

## The Year Ahead

| | | |
|---|---|---|
| **44th Annual Conference** | April 19 – 22, 2015 | Hyatt Regency Hotel<br>Atlanta, Georgia |
| **Fall Seminar** | October 25 – 28, 2015 | Hyatt Regency Hotel<br>Baltimore, Maryland |
| **Winter Seminar** | January 17 – 20, 2016 | Hyatt Regency Hotel<br>New Orleans, Louisiana |

### *Core Purpose and Values*

ACUTA's mission is to advance the capabilities of higher education communications and collaboration technology leaders.

ACUTA's core values are to:

- encourage and facilitate networking and sharing of resources
- exhibit respect for the expression of individual opinions and solutions
- fulfill a commitment to professional development and growth
- advocate the strategic value of communications and collaboration technologies in higher education
- encourage volunteerism and contributions by individual members

ACUTA

***Association for College and University Technology Advancement***

Winter 2014
Volume 18 Number 4

# INSIDE THIS ISSUE

THE ACUTA JOURNAL

***Publisher***
ACUTA
152 W. Zandale Drive, Suite 200
Lexington, KY 40503-2486

859-278-3338 general office
859-278-3268 fax

***Chief Executive Officer***
Corinne M. Hoch, PMP

***Editor-in-Chief***
Pat Scott, Director, Communications
pscott@acuta.org

***Contributing Editors***
Curt Harler
James S. Cross, PhD

***Advertising Sales***
Amy Burton, Director, Strategic Relationships

***Submissions Policy***
*The ACUTA Journal* welcomes submissions of editorial material. We reserve the right to reject submissions or to edit for grammar, length, and clarity. Send all materials or letter of inquiry to Pat Scott, Editor-in-Chief. Author's guidelines are available on request or online at www.acuta.org.

The opinions expressed in this publication are those of the writers and are not necessarily the opinions of their institution or company. ACUTA, as an association, does not express an opinion or endorse products or services.

*The ACUTA Journal* is published four times per year by ACUTA, a nonprofit association for institutions of higher education, represented by communications technology managers and staff.



ISSN 2151-3767

POSTMASTER, send all address changes to:

ACUTA
152 W. Zandale Drive, Suite 200
Lexington, KY 40503-2486
Postage paid at Lexington, Kentucky.

For more information: www.acuta.org
Membership and Subscriptions
Subscriptions are provided as a benefit of membership. The publication is available to non-members for $80 per year or $20 per issue. For information, contact Lori Dodson, Registration & Database Coordinator, 859/721-1658, or e-mail ldodson@acuta.org.



## COLUMNS



## Advertiser Index

THE ACUTA JOURNAL

## page 12

***Since 2005, there have been 725 major data breaches in the education industry, and we know many more go unreported.***

Steven Grant

## page 27

***...[M]ost account compromises happen not through technical means, but rather through social engineering, which, simply defined, is the manipulation of trust of an individual who is fooled into providing his or her login credentials to an attacker under false pretense.***

Nick Davis

## FEATURES

PRESIDENT'S MESSAGE

# Maintaining Security and Privacy in a Very Public World

*by Mark Reynolds*
*University of New Mexico*
*ACUTA President, 2014–2015*

## If security and functionality are at odds, who wins? Does security trump functionality? Does functionality trump security?

The University of New Mexico's (UNM's) IT security staff says, "It depends. Information security (often any security) and convenience are usually at opposite ends of the spectrum. Any device can be made so secure that no one can reasonably use it. There needs to be a balance between security, convenience, and functionality. Finding that balance is often difficult but seldom impossible."

Trying to maintain privacy on the Internet has become increasingly difficult. There are many different ways to be tracked online—cell phones, e-mails, Web browsers, search engines, and social media sites that produce digital footprints as a natural by-product of use. Most of us want balance and transparency. Rarely would anyone want a computer so locked it becomes a hassle to execute normal tasks. But while we wait for better privacy laws to catch up with new advances in technology and protect us against intrusive data-mining practices, we do what we can to avoid letting our data get in the wrong hands.

Within IT at UNM, we have started tightening down the laptops. This process has its pros and cons but eliminates the need to re-image as often due to virus attacks or end users who install software that turns into malware. As there are exceptions within our own IT department, there has to be a business case for maintaining this policy. Balancing efficiency, security, resource management, and transparency is now just a part of the process.

When what we do on the Internet is combined with other data about us, it creates a profile that can be tracked, and therein lies the problem of online privacy. So, how do you work in a hostile environment, knowing that someone or something is tracking you each time you browse? The IT departments, with their intrusion prevention (IPS) and intrusion detection systems (IDS), application- and network-based firewalls, ACL lists, and other systems, are continually monitoring, tracking, editing, and adding filters and rules to protect our universities from outside hackers. The IT toolbox also includes managed antivirus and central log collection/event correlation. But as we become smarter about protecting our working environment, the hackers are out front with new ways to cause havoc or total business failure. They may have already infiltrated our systems with slow-release viruses that will one day be released. This is a countermeasure from the day of a DNS (denial-of-services) attack— not a just-in-time disruption but a thought-out attack.

### Unique Network Security Challenges?

We store large volumes of highly sensitive information, IDs, and financial records for our staff, faculty, and students. Data centers designed in the past were built more for convenience and speed than security, so they are vulnerable and this vulnerability needs to be addressed.

Adding more firewalls and IPS systems and monitoring these flows cannot be the end of this conversation or design. Due to limited resources, many institutions do not have a strong IT security department, which is now the primary driver for all projects and services in the university's portfolio. These additional security requirements create the organization's dialog on balancing risk, costs, ease of use, and time to market. These additional security requirements have funding impacts and delays that were not considered in past IT projects or services. This is the new normal process we follow by having the security team involved from the beginning, which saves time for reviewing but does not address the additional funding requirements or slow time to market.

Another issue in higher education is a decentralized IT with its own servers, appliances, revenue resources, grants, and expectations. This adds complexities that central IT cannot overcome by itself, so we are campaigning for "the common good," using central IT versus the silos to curb not only the duplicate services but also sources that can be attacked and compromised causing network issues that can be catastrophic to the entire organization.

Wireless is another avenue that leaves universities vulnerable, with visitors expecting "open" access to campus resources. Open access assumes that the university has done its homework with network access control and the perimeter network to protect itself as well as its resources against possible internal threats from BYOD policies. Most universities still embrace the Freedom of Information laws, which is counterintuitive to the business model IT is trying to protect and will have to be addressed.

The "common good" campaign will eventually be embraced because colleges and universities are truly businesses that can lose millions of dollars if they are not able to provide services or if they lose critical data. Obviously, security is here to stay. Hackers and attackers will continue—whether for financial gain or just to create havoc—so universities have to consider security as a part of every project. Hackers have their own online groups and associations, just like ours—but for totally different purposes and outcomes.

*Reach Mark at reynolds@unm.edu.*

# Security Round Table Q&A

ACUTA's Fall Seminar included discussions at a security round table. The questions and the University of New Mexico's responses follow:

**Q. At your institution, where does network or data security governance reside? Is this an IT function, a function of the legal office, or a function of the office of risk management?**

A. Security governance is primarily handled by the information security office, but this team works closely with the office of university council, safety and risk services, the controller's office, and the various data stewards such as the registrar's office for student-related data, HR for employee-related data, the HIPAA compliance officer for medical-related information, and others as appropriate. InfoSec is occasionally involved with physical security, primarily as it relates to physical locations of information systems.

**Q. How would you characterize the perception of "security" at your institution from the perspective of students, faculty, and staff: necessary evil, simple nuisance, reality of the world we live in, or unaware?**

A. All of the above. In general, different groups, depending on their roles, will view security based on how it affects the tasks they are trying to complete. When convenience is affected, security is often viewed as a nuisance; but with all the high-profile data breaches recently (e.g., Target, Home Depot), I think information security is increasingly seen as a necessary evil and a reality of the incredibly connected world we are becoming.

Students, staff, and faculty come from a very diverse culture and a broad spectrum of backgrounds. Because our "city within a city" has many functions providing services internally and externally, there are many goals; and every person has a unique perspective on the institution. Unlike in a profit-driven corporation or a DOD-funded laboratory, there is not an institution-wide, 24/7 consciousness that we have sensitive data to protect, and many forget that their role is in information security (IS).

**Q. Is the security posture of your institution focused more on securing the data or on securing the device that is accessing the data?**

A. This is a balancing act. IS focuses on protecting the data first. In our open-campus community, there are so many different devices and levels of user awareness that end-point protection is difficult. But steps can be taken, such as offering a licensed enterprise antivirus solution to students, staff, and faculty at no charge. Our open and diverse community would not take well to complete management of devices; however, we work closely with workstation management to ensure that folks with privileged access are operating on "known-good" workstations in order to reduce frequency and impact of incidents.

**Q. How would you characterize the process of gaining access to a file, system, or service at your institution? Is there a formal "requesting access" procedure that requires multiple layers of approval, or is it simply calling the *right person* who can grant access?**

A. There is a formal process in place for requesting access to files, systems, and services—a request submitted through our IT service center. In some cases it is a single layer of approval, and in others it requires multiple levels of approvals—sometimes the requestor's supervisor must approve the access, sometimes the service owner's approval is required, and sometimes it requires approval from the appropriate data steward.

Also, roles may be granted by request, subject to approval, so that authorized individuals have access to sensitive information contained in our central-record management tool. Each role has a designated approver, and there is a record of who had what role at what time. One governance body is entirely focused on the security of the system, and one function of that group is to maintain rules around those roles.

**Q. How has the news associated with security breaches at Target, Home Depot, and other institutions altered the perception of security at your institution?**

A. News of recent credit card breaches has definitely raised awareness of information security, but many people still have an attitude of "It won't happen to me," "why would they want my data?" or "I don't have any sensitive data on my device." When it comes to credit card data, people understand the threat. But when it comes to their home computers/networks or mobile devices, people think their data are not at risk because it's all "in the cloud." With all of today's interconnected devices, unauthorized access to one device may allow access to other devices or data in the cloud. Attackers can also use a device they've compromised as a jump-off point to attack other devices. When law enforcement starts tracking the attack, it appears to come from a compromised device, and the device's innocent and unaware owner could be accused of the crimes.

Absolutely, those incidents have given light to what we do and what we are trying to prevent. Also, in addition to providing the community with real-world examples of massive incidents due to "small" exposures, it has raised awareness at the student level—especially those incidents where Drop Box or iCloud password compromises led to embarrassing personal data compromises.

**Q. What does your institution do to help mediate the perceived conflict between maintaining security and enabling faculty, staff, and students to perform their duties?**

A. Academic environments are built for the open and free exchange of information. This conflicts with our role in locking down data to only the appropriate people. This is again where finding the balance is crucial. Good communications channels are the best option for finding this balance.

*Reach Mark at reynolds@unm.edu.*

FROM THE CEO

# Taking Cybersecurity Seriously

*by Corinne M. Hoch, PMP*
*ACUTA CEO*

**Show me an IT professional who doesn't take cybersecurity seriously** and I'll show you someone looking for early retirement. ACUTA members take it very seriously.

One of our speakers at ACUTA's 2013 Fall Seminar in Tampa, was John MacLean, Region IV Coordinator, Department of Homeland Security (DHS) Office of Emergency Communications (OEC). I spoke with John after his presentation, and we concluded that our two organizations, DHS/OEC and ACUTA, could benefit from exploring the potential for synergies.

The ultimate result of this conversation was the formation of a Cybersecurity Task Force and its approval by the ACUTA Board. Below you will see who has been serving on this task force for the past year as well as a description of the plans this group has for the future.

Task force members are asked to share information through articles and blog posts about cybersecurity issues related to higher ed and are helping develop a new member survey regarding cybersecurity. The purpose of the survey will be to identify the top five cybersecurity issues in higher education, the information from which can be used for *Journal/eNews* articles, webinars, and possibly in-person event presentations. All information and resources developed by this task force will be posted to the new Cybersecurity Resources webpage, http://www.acuta.org/cyber.

Other ACUTA cybersecurity efforts include a webinar presentation last year by Lisa Kaiser of the U.S. Department of Homeland Security discussing the evolution of the industrial control systems cybersecurity landscape, describing significant activities and events affecting industrial control systems and the most current threats to control systems environments observed in the last several years. Lisa provided real-world examples of the consequences of cyber incidents in critical infrastructure and outlined the most recent cyber security recommendations by the DHS Control Systems Security Program (CSSP) and the Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT).

This webinar emphasized lessons learned during recent and ongoing incident-response efforts, addressing such topics as:

- How asset owners can be better prepared to handle cyber threats by practicing defense-in-depth, developing appro-

### ACUTA Cybersecurity Task Force

**Chair**

- Brian Holley, Middle Tennessee State Univ.

**Members**

- Bruce Barrett, Comm. College of Rhode Island
- Tim Cullen, ADAPTURE
- Kim Milford, REN-ISAC
- Andrew Nichols, Univ. of Illinois at Urbana-Champaign
- William Perry, California State Univ. System
- Jon Young, Vantage Technology Consulting Group

**Ex-Officio**

- Mark Reynolds, ACUTA President, Univ. of New Mexico
- Ken Salomon, Thompson Coburn LLP
- Corinne Hoch, ACUTA CEO
- Michele West, ACUTA Dir., Professional Development

**Staff Liaison**

- Amy Burton, ACUTA Dir., Strategic Relationships

October was National Cyber Security Awareness Month, and, coincidentally, ACUTA's Cyber Security Task Force met for the first time September 22, 2014. At the inaugural meeting, then-chairman Chris Boniforti, Lynn University CIO, outlined the general direction of the task force, which includes projects such as the following:

- Cybersecurity resources site on ACUTA webpage: The task force is reviewing a shell of the Cybersecurity Resources website. The intent of this website is to make available a variety of cybersecurity and IT security resources in a centralized place for ACUTA members. In addition to having links on this page, we would like to create a member CS blog that will include member-provided content, refreshed on a normal basis. More details to come.
- Top 5 CS Issues in Higher Education: Another project the task force may undertake is a survey of our members to determine the top 5 cybersecurity issues facing higher education. The results of this survey would feed content to the CS Resources website, the *ACUTA Journal* and *eNews*, as well as our webinars and in-person presentations.
- Way for Members to Talk about Issues: The task force would also like to create a place where members can communicate collectively when dealing with new vulnerability issues they are facing.

The group is currently investigating the possibility of enlisting a liaison from the Department of Homeland Security. Details will be shared as soon as decisions are made. Members are invited to contact anyone on the task force with ideas the group might consider addressing.

priate logging procedures, practicing appropriate network monitoring, and knowing the available resources for combating this type of event

- How timely information-sharing related to threats and analysis plays a critical role in empowering and protecting public- and private-sector partners
- How spear phishing attacks are used to gain footholds into well-protected corporate networks
- How organizations can improve detection measures and evaluate all connections into their control networks

In October 2014 another webinar was presented by Ken Salomon, chairman of the Lobbying and Policy Group of Thompson Coburn LLP; Rodney Petersen, executive director, Research and Education Community Security Collaborative, EDUCAUSE; and Eric Burger, who is co-director, Security and Software Engineering Research Center at Georgetown University.

The topic for this webinar was National Policy Perspectives on Cybersecurity for Higher Education. While local culture or institutional mission might cause individual institutions to prepare and react differently to cybersecurity incidents, there are opportunities for standardizing and supporting higher education at a national level. Federal cybersecurity legislation, especially in the areas of data breach notification and information sharing, could provide incentives for better cybersecurity practices. Frameworks such as the NIST Framework for Critical Infrastructure Cybersecurity or Standards like PCI could lead to more common approaches and solutions across sectors. Cyber vulnerability and incident information sharing when supported by the right liability protections and when accessible in automated formats can lead to more actionable intelligence. This webinar provided an overview of national initiatives and opportunities that can improve cybersecurity on campuses throughout the country.

### What's in It for You?

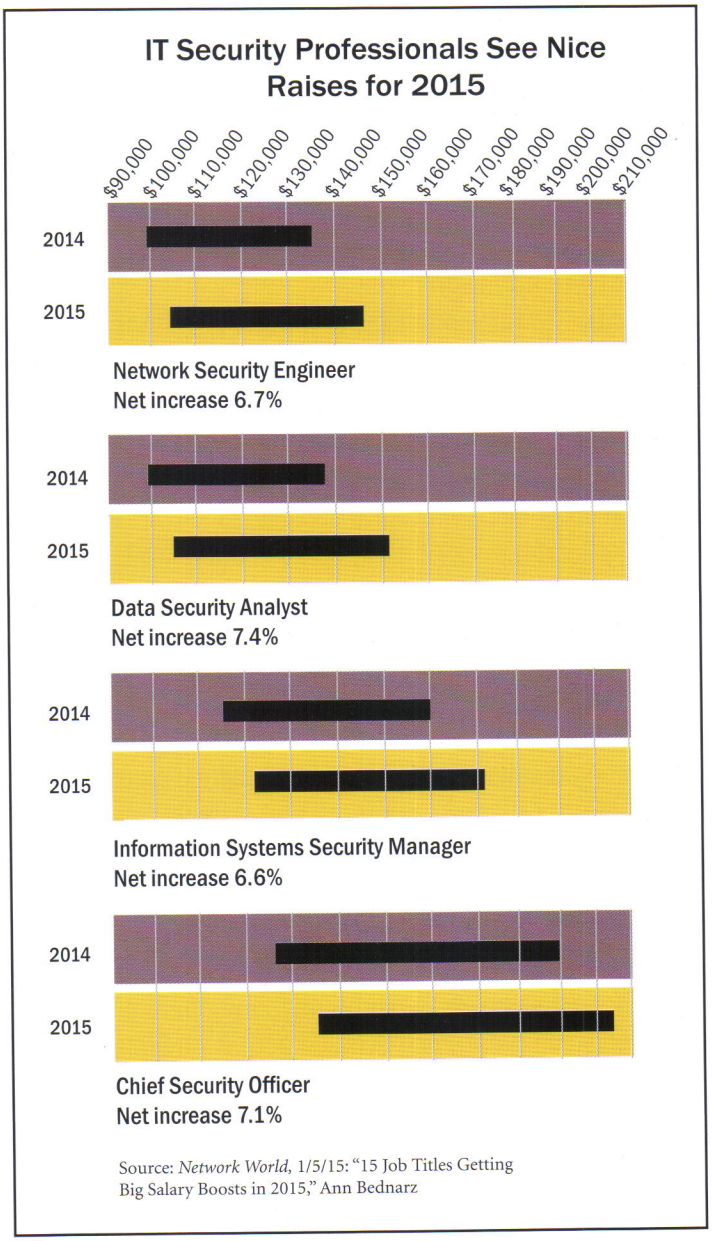
Both of these webinars, "The Evolution of Control systems Security Brief" and "The National Policy Perspectives on Cybersecurity for Higher Education," are available online. You may order video streaming of an archived version from the ACUTA Store. We encourage you to check out this valuable information as well as other resources ACUTA's newest task force will be offering in the future.

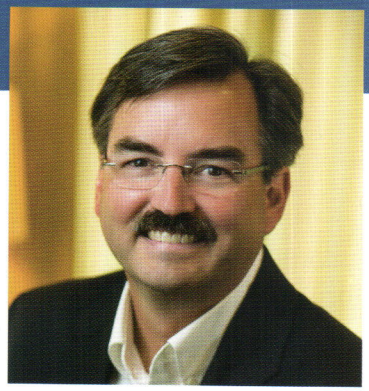
ACUTA cybersecurity efforts are helpful for our membership. As the salary increases suggest in Figure 1, keeping data safe is increasingly valued in industry as well as in higher education. Those who have never been involved in a data breach are probably in the minority. I have been involved in at least two myself. In planning the exclusive 2015 ACUTA Leadership Strategic Forum, each member of the Higher Education Advisory Panel affirmed that it is well accepted that it is not a matter of *IF* a data breach will occur, but *when*. Are you prepared? Let the ACUTA Cybersecurity Task Force help you.

*Want to know more about the exclusive 2015 Strategic Leadership Forum? Reach Corinne anytime at choch@acuta.org.*

•

*Figure 1. IT security professionals in idustry are typically receiving significant raises for 2015, indicating the increased importance of their role in keeping data safe.*





# AVST Elevates the Capabilities of Microsoft Lync

**Q&A with Tom Minifie, Chief Technology Officer, Applied Voice & Speech Technologies, Inc. (AVST)**

**Q. What are you seeing in the education market in terms of Lync adoption?**

**A.** The transition to Microsoft Lync is a trend impacting the education communications landscape. Today many of our customers have already adopted Lync for IM and presence, while some are using conferencing and voice. However, since the release of Lync 2013, there has been an escalation of interest around deploying Lync Enterprise Voice as an addition to, or as a replacement for, our customers' PBX infrastructures.

**Q. What does AVST offer to Lync customers who are in the education sector?**

**A.** AVST's CX-E offers the broadest interoperability suite in the communications industry to address two types of Lync Enterprise Voice customers that exist today: those looking to integrate Lync into their existing call control environment and those doing a complete "rip and replace" of legacy PBX infrastructure in order to deploy Lync. AVST provides unified call processing across a mixed and evolving PBX environment and offers a centralized voice messaging solution across multiple locations and platforms.

**Q. What specific problems does AVST solve for Lync customers?**

**A.** AVST's CX-E offers a number of distinct capabilities that assist in the move to using Lync Enterprise Voice:

- **Compliance** – If you want different retention policies for voicemail and email, CX-E is the only independent voicemail system for Lync that allows you to keep voicemail out of Exchange.
- **Confidentiality** – If you want to restrict forwarding of voicemail outside of your institution, or want to keep messages private, CX-E provides a number of tools that make this possible.

**"Lync 2013 becomes more viable as a PBX replacement with AVST's CX-E. CX-E offers alternatives for voicemail storage while still offering a variety of mobile, web and desktop client applications."**

*– Dave Michels, Senior Analyst at Wainhouse Research*

- **User Training** – To avoid having to retrain your users on new voicemail commands, CX-E offers robust Telephone User Interface (TUI) emulations.
- **Automated Attendant** – CX-E provides a campus-wide and departmental speech and DTMF automated attendant supporting different time zones, work hours, holidays, etc. CX-E also offers IVR and notification.
- **Informal Call Center** – CX-E offers TeamQ™, a cost-effective informal call center with robust features including ACD, UCD, agent desktop control and informational screen pops, a supervisor interface and more.
- **Centralized Voice Applications** – CX-E connects Lync to other PBXs by offering 400+ telephony integrations – from traditional TDM to IP.

**Q. What is AVST's relationship with Microsoft?**

**A.** AVST has been a Microsoft Partner for more than 10 years and recently became a Lync ISV Application Partner. As Microsoft becomes a more dominant player in the unified communications space, AVST is excited to be part of the Microsoft Lync ecosystem and keeping our education customers at the forefront of the UC industry.

For more information, visit **www.avst.com/lync**

# Privacy Matters

## With the power to access sensitive information comes the duty to secure it

*by Geoff Tritsch & Jon Young*

What is privacy? In a world where Netflix knows your taste in movies, Spotify and Pandora offer uncannily accurate suggestions about what music you'd like to hear, and your local grocery store knows what you had for dinner last week, the concept of "privacy" has changed dramatically.

We may not be able to describe exactly what constitutes privacy these days, but most people can tell you what it feels like when it's been invaded. People of different cultures, customs, and nationalities may have widely varying expectations about what privacy is and what it should apply to, but most everyone agrees that certain information should remain strictly private.

Technology has changed dramatically, and the ways in which privacy is protected—and violated—have changed right along with it. Conversations have always been vulnerable to eavesdropping; letters have been steamed open for centuries; phone calls can be monitored. But in the age of technology, such invasions have given way to more sophisticated intrusions. Text messages can be intercepted; computers can be hacked; identities can be stolen; credit card numbers can be acquired—sometimes en masse. Any discussion about technology quickly touches on issues of privacy, and modern technology can't always tell the difference between good guys and bad guys. We may not even agree on who the good and bad guys are.

### Our Lives Are Online

With so many routine tasks such as banking, shopping, and paying bills moving online, identity theft has become one of the 21st century's most troublesome crimes. There has always been a battle between those who want to maintain privacy and those who want to exploit vulnerabilities for their own ends. That battle has moved into cyberspace. The legal landscape is constantly adapting, yet it never quite catches up with technology's rapidly evolving capabilities. Complex and sometimes conflicting laws and regulations must be upheld by the various organizations and business concerns entrusted with protecting private information. Combining the legal landscape with our perceived ethical obligations is far easier to say than it is to do.

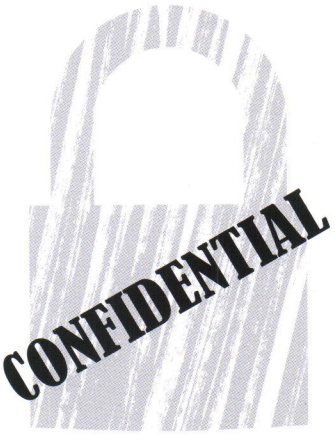
Privacy, security, confidentiality—these are the issues of the modern age. The public's right to know versus the individual's right to control. The Internet's insatiable hunger for information versus every individual's right to privacy. Organizations want to prosper and grow, and our society thrives when our education and commerce do.

Education and commerce have moved online, and security breaches pose a threat for educational institutions, business entities, and individuals alike. These complex issues and intertwined concepts must be better understood—and addressed. A good place to start is to consider the terminology we use to discuss them: privacy versus confidentiality versus security.

### Defining Our Terms

In simple terms, privacy applies to people, confidentiality applies to data, and security is the effort we put forth in order to maintain confidentiality. Sounds simple enough, but these terms can quickly get confused, especially when we define one in terms of another. Privacy consists of confidential information that must be kept secure. But the concept of what is private is complex—and malleable—often changing with each new situation and context.

For example, let's say that I consider my salary to be private. I choose to share that information with my spouse, my accountant, my financial planner, and various governmental entities that compel me to reveal it. I nonetheless choose to keep it confidential from my colleagues, my family, and the rest of the world—and I expect those with whom I share it to do the same.




However, if I were employed by certain state agencies or institutions, I might be compelled to reveal my salary as well as other "private" information. Though I would prefer confidentiality, the laws of the state employing me may override my preferences. On the other hand, maybe I make a great salary and like to brag. Same information; different context; different requirements and results.

As educational institutions, we have access to a broad range of information that *must* remain confidential, a broader pool of information that *should* remain confidential, and an even broader set that might be considered private. Volumes of potentially confidential information pass through the networks and phone systems we manage every day, and we typically have the power to access that information with ease.

*Table 1. Institutions often require potentially sensitive data for specific goals.*

| Function | Data Collected |
|---|---|
| Recruit and admit students (admissions cycle) | Name, grades, school and extracurricular activities, address, parents' names |
| Provide financial aid | Detailed financial and tax information for student and parents |
| Campus parking | Billing information, where and when someone arrived on and left campus |
| WiFi network connectivity | Device identifiers, precise location and movements, websites visited |
| Telephone service | Precise location, contact, when and with what frequency |
| Recruit, retain, pay, and provide benefits (HR) | Family names, ages, SSN, gender, health conditions, employment status, contact information |

We can't refuse to accept private and proprietary information. It is a basic necessity for many functions on campus. Examples of institutional functions requiring the collection of private data and examples of potentially sensitive data associated with those goals include what is shown in Table 1. Consider these data in aggregate—we could know exactly where each person was on campus at any given time; what websites they visited; when and for how long they were online; who they communicated with; how much money they make; what financial institutions they bank with; their spouse's name; their sex, age, family health history, childhood activities; and more—and we could correlate it all into an accurate personal profile.

### Quis Custodiet Ipsos Custodes?

As the owners and operators of enterprise systems that collect such data—and the networks over which information passes—we have a tremendous responsibility to protect this information, even as we perform the following multiple and sometimes competing roles:

- Maintain the confidentiality of our institution's data
- Assist our users in keeping their data confidential
- Maintain the privacy of individuals from whom and about whom our institution collects data.
- Ensure the effective operation and security of our network and systems.

Our ability to maintain privacy is contingent on our ability to secure confidential information and keep our networks secure. But our ability to keep our systems and networks running effectively and to keep the network secure requires monitoring the (often private) information that crosses our networks. We have to trust that those who watch the network are more interested in maintaining its integrity than in the information running across it—a dynamic that leads to this age-old question: Quis custodiet ipsos custodes? Who watches the watchers?

### Consider What You Collect

With ever-greater amounts of confidential data being generated, the need for a privacy policy is beyond question. Yet, remarkably, few institutions actually have one in place. And for those that do, those policies often fail to encompass the full spectrum of privacy related issues.

Key to the effectiveness of any privacy policy is the need to strike a balance between institutional needs and the potential impact on everyone's privacy in the event of a security breach. Our natural inclination is to collect and retain everything. But even seemingly innocuous information can create privacy issues when revealed or mined, especially in combination with other seemingly innocuous information.

Could a seemingly "safe" piece of information be combined with other similarly "harmless" bits of data to ultimately expose information someone considers confidential? And if that's possible, does the potential future value of institutional data collection outweigh the risk of an invasion of personal privacy? Would the person whose privacy is in question give a different answer? The answer to these questions may trigger another: Should we limit data collection to those areas that have specific and immediate value?

If some of the data being collected has no immediate value, is it worth the potential privacy risk to collect it? Why collect it at all? We need to carefully examine these issues, the potential privacy implications, and the institutional risk were that data to be breached or used in some inappropriate or illegal way.

How long should we retain the data we collect? When and how do we purge data that is no longer necessary? For example, if we compile call detail records (CDRs for billing and fraud purposes, should we purge that CDR data after the bills have been paid and some reasonable period of time has gone by to contest those bills? CDR data clearly has potentially confidential information in it, such as calls to or from mental health facilities, family planning clinics, divorce attorneys, and more.

These important considerations must be addressed by any organization responsible for maintaining and operating data-rich online systems. The educational community must stay ahead of the curve as even more functionality and sensitive information migrate online.

### Privacy Impact Assessment

One way institutions can answer these important questions is by creating a privacy impact assessment (PIA). This worthwhile tool identifies and assesses the privacy risks that exist when an organization collects, uses, shares, and stores any individual's personal information. PIAs provide a process to assess the privacy ramifications of data collection and ensure that security protocols effectively support the privacy policies, regulations, and compliance goals of the institution.

There are many examples of PIA methodologies available online. However, if you do a Web search for *privacy impact statement,* you will quickly see that the phrase lends itself to a wide array of applications and implementations. Yours need not be onerous. By adapting the examples online and overlaying your institutional culture, you can create a process that will serve your organization in a clear and straightforward manner.

As with so many other discussions about defining and achieving institutional goals, this brings us back to setting and maintaining policy. A privacy policy should set expectations for both the data collector and the "owner(s) of the data." The expectations for all parties should be a privacy policy that is:

- Reasonable
- Clear
- Agreed upon
- Articulated
- Documented
- Auditable

We in IT often fail in one or more of these areas, but the auditable element is probably the most difficult to implement. Consider that many of us have negotiated into third-party contracts that contain provisions about how our institutional or end-user data will be managed. Examples might include the common provision in the Google Apps for Education environment, assuring us that our user's e-mail will not be mined for any purpose. How do we audit that obligation?

That question was recently posted on the EDUCAUSE CIO mailing list, generating a variety of interesting responses and a number of further questions. To turn the question around, if we create rules that say we won't retain certain types of data, that we will restrict who has access to what we retain, and that we will purge data after a specified period, what controls have we implemented to ensure that these obligations are being met, and how can we audit that?

### From CISOs to CPOs

By now many (most?) institutions have a chief information security officer (CISO), be it full-time with a staff, a solo effort, part-time faculty, or shared with other institutions. Few institutions of higher learning—except for some of the largest—have a chief privacy officer (CPO). But aside from sheer quantity of information, privacy issues bear little relationship to institutional size.

The role of the CPO should be to assist in raising awareness, develop institutionally appropriate policies, and act as the advocate for privacy for the campus. Given the nature of the role, it may be appropriate to recruit a faculty member with subject matter expertise as a part-time CPO. Despite the potential conflict of interest, we have even seen some institutions tap their CISO as the CPO effectively.

### Conclusion

As an independent consulting firm specializing in the strategic application of technology in higher education, healthcare, and urban media, Vantage holds the overarching view that privacy must be viewed from the context of what is:

- Legally mandated
- Ethically appropriate (not always in agreement with the law)
- Supportive of the institutional mission
- Appropriate to the campus culture

Historically, and for a number of practical reasons, IT personnel have often made decisions about what their institution should do regarding privacy. Those decisions were often based on what best fit the operational goals and limitations of the IT group. This can no longer be the case. Privacy is an institutional governance and cultural issue. IT should serve as an implementer and adviser, certainly, but should not be setting policy. IT must retain its key role of being the subject matter expert, a strong privacy advocate, and the potential driver in encouraging institutional leaders to consider privacy objectives and policies. But the stakes are too high and the costs of failure too dear to have IT go it alone when privacy matters so much.

*Geoffrey C. Tritsch is a principal with Vantage Technology Consulting Group. An expert in the unique voice, data, and video needs of large, nonprofit organizations, he has worked in the telecommunications industry for more than 35 years. Geoff can be reached at Vantage's Boston office at 978-610-3805 or at geoffrey.tritsch@vantagetcg.com.*

*Jonathan Young is a senior consultant with Vantage Technology Consulting Group. Jon has over 19 years of experience managing IT systems, networks, and departments. Jon is platform agnostic and focuses on building groups, systems, & networks with a risk-informed approach to reliability, disaster recovery, and scalability. Jon can be reached at 978-610-3812 or at jonathan.young@vantagetcg.com.*

*Special thanks to Tim Barkas, also of Vantage, for his excellent editing.*

•

# Crisis on Campus

## Security concerns threaten to rob IT budgets, stalling service growth

*by Curt Harler*
*Contributing Editor*

Data breaches are having a devastating financial impact on the education community. Security is costing colleges so much money that IT managers are being forced to make unsavory decisions about whether to allocate budget dollars to upgrades and user services or simply to prevent data breaches and hacking. It's a bit like trying to decide which one of your children to rescue from a fire.

The increased adoption of mobile, social, and cloud computing is driving growth in security spending among organizations that are also becoming more aware of threats on all those fronts. Worldwide spending on information security topped $71 billion in 2014, an increase of 7.9 percent over 2013. The data loss prevention segment recorded the fastest growth at 18.9 percent, research firm Gartner said in a study released in late August 2014.

Gartner's research director, Lawrence Pingree, points to what he calls the "democratization" of security threats, with malicious software tools that can be used to launch advanced attacks now more broadly available online via an underground economy. While this has made life even more difficult for IT security, it has also resulted in increased awareness. Security is no longer seen as just an IT function or a cost center, he says. He sees organizations shifting existing resources away from security device administration and monitoring and toward mitigation and incident response.

At Valparaiso University, Bob Konicke, director of network services, finds their hard costs for security are low. "But," he adds, "staff time can be extensive during peak phishing 'storms,' which is the most prevalent issue here."

Barron Hulver, director of networking, operations, and systems at the Center for Information Technology at Oberlin College, has the same complaint. "IT security is something we put a lot of energy into," he says. "We put a lot of people-time and money into it, and there is no return on it." By that, he clarifies, he means there is no real benefit to the user community in terms of improved services. Like insurance, there is a payback only if we need it. "We spend an inordinate amount of time maintaining interior and perimeter firewalls, logging events, and updating patches. However, in one way it probably is money well spent. Since 2012, 20 percent of all U.S. data breaches took place in the education sector."

"Since 2005, there have been 725 major data breaches in the education industry, and we know many more go unreported. Few schools budget for the unexpected expense of a data breach, and few have the technology in place to prevent it. The education industry needs a secure solution for protecting its students, faculty, and staff from hackers," says Steven Grant, vice president of operations for EduLok, an affiliate of the Manchester, New Hampshire–based WWPass Corporation. "More than just a financial issue, a data breach puts a school's reputation at risk."

Some sources suggest that a typical breach may cost more than $10 million. Other reports are considerably more conservative. A survey of 3,529 IT and security practitioners by the Ponemon Institute found that most (32 percent) malicious breaches cost between $500,000 and $1,000,000 each, whereas most (22 percent) nonmalicious breaches cost between $50,000 and $100,000 each. In the United States, it takes 92 days for an organization to recover from a nonmalicious breach incident and 125 days to recover from a malicious breach incident, from the time of discovery to full resolution.

Many ACUTA members feel a bit like the Christians in the Colosseum: nearly naked in the face of a ferocious foe. The Ponemon study reflects that helplessness: Only 40 percent of IT and security professionals said they have tools, personnel, and funding to determine the root causes of network security breaches. For nonmalicious attacks, when IT and security professionals were asked why they were unable to prevent the breach, 50 percent said lack of in-house expertise and 37 percent said inadequate security procedures.

Indeed, most network security breaches are inside jobs. Statistics show that 61 percent of data and security breaches are from employee negligence and malicious insiders. But that does not mean the bad guys are cutting the good guys any slack.

"Network security issues are not going away anytime soon, and by most measures they are multiplying on a daily basis," says Dan Williams, enterprise

account manager with XO Communications. He says it is imperative that enterprises of all sizes put in place a comprehensive, managed, network-based approach to ensure 24/7 protection from the increasing number of network threats. "Doing this," he says, "will enable you to focus on your core business and not be losing sleep at night worrying about the myriad risks your business faces by not addressing this very real issue."

### You Are Under Attack!

Advanced persistent threats are highly organized, well-funded, multivectored cyberattacks that target specific organizations. Using different methods, attackers will relentlessly attempt to gain access to the college's network and will remain there for a long time, until they have achieved their objective.

There are many examples of these massive attacks, with the most prominent being the Stuxnet targeted attack on an Iranian nuclear power plant and Operation Aurora, which targeted intellectual property and user account information in Google, Adobe, Rackspace, Juniper Networks, Symantec, and many other high-profile organizations.

The malware commonly used in these types of advanced attacks is simply a tool for the collection of data. Sophisticated hackers are using different pieces of code for each phase of their attack, making detection of these advanced attacks problematic, according to Canalys, a high-tech consulting firm with offices in Palo Alto, California, and Reading, United Kingdom.

If you are looking for an ally in the battle, there are a handful of specialist vendors in the market, including FireEye, Bit9, Cyphort, Guidance Software, Damballa, and mobile forensics specialist Cellebrite, Canalys says. The reaction in the IT security market has led to many vendors creating marketing campaigns highlighting the need for advanced threat-detection solutions. While this works well for them as a tool to generate interest in their offerings and to differentiate from one another, it also creates a lot of confusion in the market for IT managers and business stakeholders, who are uncertain if these threats are merely hype and do not affect their business or if they need to carve out a budget for the right security measures, Canalys reports.

Most observers agree that security costs will be like the electric bill—continuing into the indefinite future with little chance of ending or decreasing.

"It is interesting that anybody would expect the situation to improve in the foreseeable future," Valparaiso's Konicke muses. "As is regularly demonstrated in the news, even companies with no choice but to invest in costly, labor-intensive and sophisticated systems are breached all too frequently.

"I expect that our cost will escalate in the next couple of years," Konicke says. Unfortunately, many organizations continue to lack staff with the appropriate security skills. To keep up with hackers, more than half of organizations will, by 2018, rely on security services firms that specialize in data protection and in risk and infrastructure management, according to Gartner.

To combat these threats, security vendors are introducing solutions that predominantly use signatureless technology. Examples include sandboxing, emulation, big-data analytics, and containerization. Since these threats can be network based

or endpoint based, vendors from both the network security market and content security market are rolling out solutions to tackle this threat.

### Passwords

According to security experts at Thycotic, in Washington, D.C., the top three passwords are Password1, Hello123, and password. Well, duh!

Many administrators require a mix of uppercase and lowercase letters with numbers and one or more special characters in a password. That will make it more difficult for a human to guess a password, but it will not make for a more secure password that is being machine hacked, according to Trustwave. In a 123-page report, Trustwave says a mix of uppercase and lowercase characters is not that challenging for password-cracking tools. "Only increasing the number of characters in the password dramatically affects the time it will take an automated tool to recover the password," the report says.

An automated tool can crack a completely random eight-character password, including all four character types such as "N^a&$1nG," much faster than a 28-character passphrase including only upper- and lowercase letters like "GoodLuckGuessingThisPassword." If for the purposes of this estimate we assume the attacker knows the length of the passwords and the types of characters used, "N^a&$1nG" could be cracked in approximately 3.75 days using one AMD R290X high-speed graphics processing unit (GPU). In contrast, an attacker would need 17.74 years to crack "GoodLuckGuessingThisPassword" using the same GPU.

### Encryption

"Encryption can be a blessing, or a curse if inappropriately applied," says Steve Surfaro, chair of the Physical Security Council and security industry liaison at Axis Communications in Chelmsford, Massachusetts. He says a college must first determine what type of encryption is being used and whether this encryption standard has been published and certified.

Encryption systems, also known as cryptosystems, must be validated and approved at a specific security level under a certification process known as Federal Information Processing Standard 140—which identifies the requirements and standards for cryptographic modules, including both hardware and software components for use by departments and agencies of the U. S. federal government.

"Software-based encryption is often known as a weaker type of encryption, as it is stored on media that can be extracted with less difficulty than a stronger type of encryption known as hardware-based encryption," Surfaro says. Hardware-based encryption uses a specific device known as a hardware security module (HSM), or trusted platform module (TPM), containing a cryptographic co-processor that runs completely separately from the systems processor and operating system.

Probably the most prevalent and widely used set of cryptographic standards are those published by RSA (www.rsa.com). They use the suite of standards called Public-Key Cryptography Standards (PKCS). Each standard defines a number of cryptographic processes which can perform public-key distribution, serve as cryptographic interfaces between systems, and handle signing and verifying the authenticity of private keys used in secure communications. Each standard is defined with a number, such as PKCS#1, PKCS#2, and so on.

Today, the U.S. government requires encryption and identification and authentication controls to be embedded in physical security devices. In government-speak, these are called "nonperson entities." NPEs must have a unique cryptographic key that will ensure that these devices are constantly used in a secure state while deployed.

### Final Thoughts

Regulatory compliance has been a major factor driving spending on security in the past three years, particularly in the United States, according to Gartner. Privacy and data protection laws in various stages of implementation or planning in Australia, the European Union, Singapore, and Malaysia will further help drive growth.

Much will be spent on cloud services.

The growing popularity of hosted applications and infrastructure is changing the security sector. In 2015, roughly 10 percent of overall IT security enterprise capabilities will be delivered as a cloud service, Gartner predicts. Small- and medium-sized enterprises will rely on hosted security services to an even greater extent.

Where would IT managers spend budget money if it were not earmarked for security? "That seems so irrelevant that I'm intrigued that anyone would bother asking," Konicke says.

Hulver is sure Oberlin could find a place for those funds in buying more Internet bandwidth. "Our Internet bandwidth demand curve is exponential," he says. In 2000, they had two T1 lines. "In 14 years, we went from 3 Mbs to 1 GBs," he says. He predicts they will be at 4 GBs in less than four years. In fact, they are just finishing installation of their first 10-Gig link with Time Warner Cable.

Wherever the money could be allocated, it is a near certainty that it will not be coming from the security budget. Security expenses will continue to gnaw at IT budgets like a cancer.

*Curt Harler is a freelance writer, a grand adventurer, and a contributing editor for the ACUTA Journal. Reach him at curt@curtharler.com.*

# Appropriate and Reasonable Protections

## A Legal View of Data Security

*by J.G. Harrington*

Higher-education institutions have many reasons to maintain privacy of the data they create and store. This article provides an overview of the legal obligations that relate to data security at the federal and state level. It also analyzes potential legal risks, including factors that affect the level of risk, and steps that colleges and universities should—and should not —take to address data security risks.

### Federal Law

The primary sources of data security obligations under federal law are the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and the regulations of the Federal Trade Commission (FTC). In addition, under a February 2013 executive order, the federal government has created new programs for informing targets of cybersecurity threats and a cybersecurity framework to provide guidance to private entities in developing cybersecurity practices.

- FERPA

FERPA is the basic education privacy law. It covers educational information, including records, files, and other materials; personally identifiable information (generally known as PII), including name, family member names, address, personal identifier, birthday, and place of birth; and directory information, which is PII that is not sufficiently private that it must be protected, including name, address, phone, e-mail, birthday, photos, major, degrees, awards, and sports-related information.

Under FERPA, use of protected information is limited. The primary use is for legitimate, education-related purposes, which covers most of what a college or university would do with the information. Protected information also can be released or used in response to subpoenas and court orders, to maintain health and safety, and to support juvenile justice. The restrictions on directory information are much less stringent, but use and release of that information are subject to the student's right to opt out.

FERPA is enforced by complaints to the Department of Education, and violations can jeopardize federal funding. The courts have not permitted individual lawsuits under FERPA for damages.

- HIPAA

HIPAA creates privacy rules for health-related data. It applies only to "covered entities" and protects "individually identifiable health information."

Individually identifiable health information is information concerning someone's health status, the healthcare that individual receives, and payment. This information can be disclosed only in accordance with the federal Department of Health and Human Services (HHS) HIPAA rules or with written authorization.

Covered entities fall into three categories: health-care providers, health plans, and healthcare clearinghouses. In general, colleges and universities are healthcare providers through affiliated hospitals and clinics (including on-campus health clinics). HIPAA applies to healthcare providers only if they transmit information in electronic form in connection with a transaction for which HHS has created a specific standard. Any covered entity has a duty to identify and protect against reasonably anticipated threats to the security or integrity of healthcare information. Thus, both disclosure of covered information and threats that could alter or delete that information are within the scope of HIPAA. HIPAA preempts inconsistent state laws, but there are some exceptions.

HIPAA is enforced through complaints to HHS. There are penalties for willfully neglecting HIPAA obligations and for failing to correct violations within 30 days of when the covered entity should have known of the violation. These penalties range from $100 to $50,000 per violation, up to $1.5 million per year.

***If policies and practices are left in place for an extended period without review and revision, they may no longer be adequate or suitable, which increases legal risk in the event of a breach.***

- FTC

The FTC has wide-ranging authority over commercial practices in the United States. Its authority comes from multiple sources including the Fair Credit Reporting Act, which generally applies only in the context of credit reporting; the Children's Online Privacy Protection Act, which limits collection of personal information from children under the age of 13; the Gramm-Leach-Bliley Act, which covers financial products and services; and the FTC's general fair trade practices authority.

While the FTC generally has not enforced privacy and data protection requirements against colleges and universities, it has been interested in these issues as they affect the broader marketplace. To that end, it adopted best practices in 2012. These best practices are built around three principles:

- Privacy by design: Addresses privacy throughout the product development process.
- Simplified choice: Consumers decide how their data will be used at relevant times and in relevant contexts.
- Transparency for information collection and use: Ensures that customers understand what is done with their information.

These practices are not mandatory but provide guidance on how to approach privacy and data protection.

- Administration Data Initiative

In February 2013, President Obama issued an executive order on cybersecurity. The order had three elements. The first element was to have U.S. law enforcement and national security agencies report cybersecurity threats to identified targets, where doing so would not jeopardize ongoing investigations or national security.

The second element was to expand Enhanced Cybersecurity Services, a voluntary federal program that facilitates information sharing, to a wider range of critical infrastructure operators.

The third element of the executive order was the creation of a voluntary framework to reduce risks to critical infrastructure, focused on standards, methodologies, and procedures and incorporating consensus standards and best practices. This framework, which was released in February 2014, has three key elements:

- The framework core, built around the basic functions of addressing threats: identify, protect, detect, respond, and recover
- Implementation tiers, which are four levels of response, ranging from informal and reactive to agile and risk-informed
- Profiles, which look at specific functions and activities to determine whether current protection is sufficient and to set appropriate action plans

The framework creates a set of principles for evaluating not just threats but the extent to which resources should be directed at protecting individual activities. While the framework expresses a preference for active approaches, it also acknowledges that it is not appropriate to adopt the highest implementation tier for every type of activity. Although the framework is voluntary, it is intended to create a set of best practices for addressing cybersecurity issues.

> As we know,
> There are known knowns.
> There are things we know we know.
> We also know
> There are known unknowns.
> That is to say
> We know there are some things
> We do not know.
> But there are also unknown unknowns,
> The ones we don't know
> We don't know.
>
> *— Donald Rumsfeld, February 12, 2002*
> *Department of Defense news brief*

- Federal Legislation

At the very end of its 2014 session, Congress passed the National Cybersecurity Protection Act of 2014. This law will codify the existing cybersecurity program in the Department of Homeland Security, which facilitates information sharing on cybersecurity. The law does not, however, provide anonymity for stakeholders participating in the program and does not include any liability protection for participants who reveal data breaches. These omissions reduce the likely effectiveness of the program and leave existing legal risks unchanged.

### State Law

State law concerning cybersecurity varies widely. The most common laws address security breaches, but some states also have laws concerning online privacy and privacy of employee communications. In addition, state common law—that is, law made in courts via lawsuits—can have an impact on cybersecurity.

According to the National Conference of State Legislatures, 47 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have laws requiring notification of data breaches. These laws typically define what types of entities and information are subject to the notification requirement; specify when a reportable breach has occurred; and define who gets the notification, how it is delivered, and when it must be sent. Even within these parameters, requirements can vary widely. For instance, sometimes notices go to the government, sometimes they go to affected parties, and sometimes they go to both.

Other common state laws govern online privacy and employee communications. California and Connecticut require privacy policies for all online services, and 16 other states have online privacy laws that cover government sites, including sites of state educational institutions. At least two states, Nebraska and Pennsylvania, have laws that prohibit

false or misleading statements in online privacy policies. These online privacy laws may apply to online courses in some cases. Connecticut and Delaware require notices to employees when their communications are being monitored, and Colorado and Tennessee have similar laws that apply only to public employees.

Data breaches continue to be of interest to lawyers who file class action and personal injury cases and who often base claims in the common law. These suits usually are based on theories of negligence, breach of contract, or breach of fiduciary duty. Although lawsuits based in common law generally have not been successful to date, the cost of defending such suits can be significant.

### Assessing Legal Risks

There is no simple formula for assessing the legal risks associated with data security. There are, however, some approaches to thinking about these issues that can help in determining appropriate priorities and what resources should be devoted to specific solutions.

The most significant risks arise from data subject to specific protection under the law, where there is a clear duty to protect the data and where the impacts of releasing the data are greatest. Consequently, the greatest risks come from data protected by FERPA or HIPAA and from financial data, whether it is institutional or individual information. Conversely, legal risks are lower, in general, for internal e-mail or information that is made available on an institution's website or sent via that website.

Legal risks also may depend on the nature of the information and how it is used. Risks are greater when there is an obligation to keep the data private or some other expectation that the data will be protected, but it may be lower if there is an understanding that many people will have access to the data or if people outside the institution will have access. Risk also is affected by the potential impact of the disclosure—including financial impacts, potential embarrassment, or other nonfinancial harm that could be caused by disclosure.

In addition, legal risk is affected by the steps the institution has taken to protect the data. Lax security practices (particularly for access to administrative functions), a failure to recognize the specific security needs for particular types of data, and the failure to follow established policies will increase legal risk. Consistent implementation of policies and practices adopted by the institution and implementation of best practices and standards (including changing practices and policies as standards evolve) will reduce the legal risk if a breach occurs.

### What Can Be Done

In many respects, the best approaches to minimizing legal risks from data breaches are similar to the best approaches to maintaining communications networks, which require ongoing attention and adjustment as circumstances change. The worst thing to do is nothing, particularly as attacks become more frequent and more sophisticated.

In broad outline, the following steps will help minimize an institution's legal risk:

- Develop and implement appropriate security policies: Policies should be based on established best practices and should be differentiated based on the specific risks for particular types of data.
- Develop specific processes for responding to security issues: These processes should include the internal steps that will be taken and any external communication, notification, or outreach.
- Involve the institution's internal counsel and risk management department throughout the process of developing and maintaining policies and practices.
- Evaluate policies on a regular basis: What constitutes adequate security is an evolving standard. In addition, new or changed services may require new security measures.

There also are actions (or inactions) that institutions should avoid. While security policies and practices may draw on what others have done, an institution's risk is increased by wholesale adoptions of the practices of other entities without evaluation of how those practices fit the institution's needs. Similarly, if policies and practices are left in place for an extended period without review and revision, they may no longer be adequate or suitable, which increases legal risk in the event of a breach. Finally, if a breach does occur, risk is increased if the institution tries to hide the breach or applies a superficial fix without working to implement a more comprehensive solution.

### Conclusion

While there is no way to eliminate the legal risks of a data security breach—just as there is no way to eliminate the risk that a breach will occur—there are strategies that can reduce those risks and protect both the data and the institution. By adopting best practices adapted to the institution's specific needs and by evaluating and revising those practices over time, an institution can address and minimize the potential for legal liability if a breach occurs.

*J.G. Harrington is currently special counsel at the Washington, D.C., law firm of Cooley LLP. He has represented telephone, mobile communications, cable television, and new technologies clients on federal and state regulatory issues and has worked with other clients to address issues that arise in their interactions with service providers and regulators. He has developed special expertise in matters relating to telecommunications competition, regulatory issues affecting new technologies, broadband services, privacy, intercarrier compensation, universal service, telephone interconnection, and telephone and cable rate regulation. Reach J.G. at jgharrington@cooley.com.*

•

# Securing the Cloud: Key Contract Provisions for Institutions

## Keeping your institution's data safe requires diligence on your part

*by Joe Dysart*

While untold numbers of colleges and universities are saving money by moving to the cloud, IT experts say these organizations need to ensure their cloud contracts include ironclad security protections—or they'll suffer an uncertain future.

"Look at the news on any given day," says Ron Zalkind, chief technology officer at CloudLock, a service provider that helps organizations secure public cloud accounts like Google Apps and Salesforce. "You'll clearly see that the number of risks and data breaches is only accelerating," says Zalkind.

Moreover, getting from "uncertainty" to "protected" can be more difficult than you might expect, given that many cloud-service providers are reluctant to put their security assurances in writing.

"We continue to see frustration among cloud-service users over the form and degree of transparency they are able to obtain from prospective and current service providers," says Alexa Bona, a managing vice president at Gartner (www.gartner.com).

Not surprisingly, the cat-and-mouse game between user and cloud provider is taking a toll. Many organizations are simply delaying a move to the cloud due to their concerns over security, according to a 2014 study released by Bitglass (www.bitglass.com), a cloud security firm.

Specifically, Bitglass researchers found that more than half of large-sized organizations (52 percent) and approximately one-third of small- to medium-sized organizations (33 percent) cite security as their primary concern when it comes to cloud-based IT.

Plus, the percentage of organizations concerned about cloud security is increasing, according to the Bitglass survey. While 25 percent of companies expressed security concerns in October 2011, the figure increased to 42 percent in July 2013, according to Bitglass researchers. Even so, many institutions find the siren call of cloud IT hard to resist. "Sure, there are news reports about cloud breaches—but there are plenty of examples of large-scale, on-premise compromises as well," says Joshua Beeman, university information security officer at the University of Pennsylvania.

"The most popular cloud services dedicate hundreds of millions of dollars—and thousands of people—to the secure and robust delivery of their product," Beeman adds. "Many of us do not have the same luxury or dedicated resources."

### Standards and Guidelines

Fortunately, federal governments are stepping in to help assuage concerns. EU regulators, for example, are aggressively pushing for more detailed cloud-security agreements between providers and universities. The EU rolled out a set of guidelines in 2014 worked out with key global cloud-service providers such as IBM, SAP, and Microsoft. (https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines)

"A competitive digital single market needs high standards of data protection," says Viviane Reding, vice president of the European Commission, who adds that the new guidelines are a step in the right direction.

Similar efforts are underway in the U.S. National Institute of Standards and Technology (http://collaborate.nist.gov/twiki-cloud-computing/bin/view/Cloud-Computing/WebHome). Essentially, the standards—which will apply to cloud-service providers doing business with the federal government—are expected to serve as best-practice cloud security contract templates for all of industry in the United States.

Sean Moriarty, chief technology officer, Campus Technology Services, at State University of New York at Oswego, says "When you have the right partners, the risk of placing your data in the cloud versus having it on campus is comparable or can be lower."

Of course, despite hoped-for government protections, it's always good sense to make sure provisions for the security of your data are made explicit before you ink any cloud contract. Here's what cloud-security experts recommend (consult with your institution's legal staff before implementing any contracts):

- Be sure there are limitations on where your data will be geographically located. Nail this down, or your institution's data could end up on a server in Iran.
- Be sure you have a detailed exit strategy from your cloud-services provider. Should you decide to move on to another provider, you'll want to be sure there is clear agreement on the transition.

Specifically, nail down how you'll move your institution's data. You'll also want to nail down the data format in which your data will be sent to you for the transition. You'll also want in writing the kind of cooperation your old provider will give you and the amount of time you'll have to secure your data. Otherwise, with nothing in writing, your institution could simply lose all its data with a move.

- Beware of cloud providers that insist on the unilateral right to change contract terms. Essentially, this right can give your cloud-service provider a blank check to make changes to your contract terms on a whim—and leave your data in the lurch. If the provider refuses to budge, be sure you can live with this provision.
- Get documentation on how your provider will secure your data. Any decent cloud provider will have internal protocols in place designed to safeguard your data and your institution's privacy. Get those protocols in writing. And get a guarantee that your provider's security standards will be certified annually.
- Get documentation that your provider is aware of all local, regional, national, and international laws regarding the security and privacy of your data. And get documentation and descriptions of the systems your provider has in place to comply with those laws. Also, get similar documentation that your provider is aware of and can comply with laws that are specific only to colleges and universities.
- Ensure that your provider will be able to provide usable data should your institution be faced with an eDiscovery request during litigation against your institution. Your legal staff should know how to ensure this request is properly fulfilled.
- Ensure that the cloud contract clearly states that your institution retains ownership over all its data and that the cloud-services provider has no right to use your data. Otherwise, the cloud provider may try to resell your data to third parties.
- Ensure that your legal agreements extend to the subcontractors hired by your cloud provider. This is an easy provision to overlook and could wreak havoc on your contract with your provider if forgotten.
- If possible, ensure that your IT director will be able to meet with the cloud security chief to evaluate the provider's security protocols. Also ensure that your IT director will get immediate notice when any changes are made to those security protocols.
- Ensure that you will be notified if your cloud provider suffers a security breach or is hacked in any way. As we've all discovered the hard way, cloud providers are often reluctant to inform clients that they've been breached.
- Ensure that you're able to encrypt your data before it leaves your institution's computers. This provision can save untold headaches. Once encrypted, your data become much less of a problem for your institution in the cloud, no matter what goes on there.
- Ensure your data will be wiped clean from servers and other computerized storage devices that are taken out of service by your cloud provider. Otherwise, a server or external hard disk with all your institution's secrets could pop up on eBay and be sold to a pimply faced 15-year-old—or worse.
- Secure a detailed agreement on how your provider will handle a system crash involving your data. Also secure an agreement on how a security breach of your data will be handled. Don't assume your cloud provider will be diligent.
- Monitor the Cloud Security Alliance (https://cloudsecurityalliance.org) for the latest ideas and developments in cloud security. Its specific mission is to work on establishing international standards for security and privacy in cloud-service agreements.

*Watson, the artificial intelligence IBM computer that bested humans on the TV show* Jeopardy, *is now available as a cloud service.*

## Conclusion

This is a complex topic that would more thoroughly be covered by a significant depth of detail. These are just some highlights. Other important aspects worthy of research and consideration include the need to recognize that requirement or purpose may influence the characteristics or conditions of the contractual language and, most important, the value of engaging legal counsel with familiarity and experience in specialized IT contracts when it's time to sign on the dotted line.

*Joe Dysart is an Internet speaker and business consultant based in Manhattan. Reach him at joe@joedysart.com. Web: www.joedysart.com.*

•

# Changing Behavior ... Changing Mind-sets

## Make the message clear if you want to bring about lasting change in security habits

*by Matt Arthur*

My son drives a truck cross country for a living and relies on his laptop for communications about loads, traffic, and so on. My son is not as IT-literate as I would have hoped. Believe it or not, however, he actually does rely on my advice and input when it comes to computers and such. Don't worry though, even at 27 years of age, he still only reluctantly admits that I know much about anything else.

Recently he asked which antivirus scanning software I would recommend for his new laptop—or should I say, fairly new laptop. He had bought it approximately 90 days earlier, and the "free" antivirus scanning software license had expired. He has listened to me enough over the years to understand he probably doesn't want to be floating around the "interwebs" without some kind of protection.

### A Difficult Answer

My response was that I don't really think he should rely on any of them. Unfortunately, the antivirus industry is a *reactive* model that waits for a virus attack then formulates ways to detect it and block it. However, so many virus and malware programs attack so quickly and constantly that the ability of the antivirus industry to react quickly and consistently enough doesn't seem to be a meaningful proposition. This is an example of using technology that worked in the earlier stages of computers-to-the-masses but not as well today.

If someone were starting out now to create some kind of protection for you while on the network, wouldn't they have to include more devices than your computer or laptop? If they started from scratch, I don't think the current antivirus and malware software dichotomy would make the cut. In addition, my son never does the updates and never wants to pay for maintenance. Over the years, I've learned that changing his behavior with better passwords or steering clear of shady links on the Web just doesn't work.

For many folks, security is something that just gets in the way and obstructs them from accomplishing their jobs or their goals. How many times does someone in IT have to do password resets due to students, staff, or faculty forgetting their latest iteration? And how many of those students, staff, and faculty would not have set up passwords of the necessary length, complexity, and unpredictability without being forced to? I'm not saying passwords are a waste of time, just that without administrative oversight, most people (especially my son) would ignore even the barest of minimum levels.

### Access without Exposure

So how can we help ensure 'they' can access technology as representatives of 'our' institutions without the constant threat of exposing our personal or institutional data to the nefarious characters that threaten us day and night? That is the question we all have to consider while doing the day-in and day-out routine of our jobs—bearing in mind, of course, that most of us are not certified, qualified, or bona fide security experts.

Let's look at how we, as bona fide information communications technology professionals in higher education, can help ensure both good security and good security practices from our students, staff, faculty, and guests.

At the ACUTA Fall Seminar this past October in Boston, one of the tracks was "Securing Our Connected Environments." I was impressed by the selection of presentations, ranging from a preconference tutorial on creating and running a successful information security program to protecting your campus WiFi and what to look for in cloud-based storage—and that was just the first day. The final session was an interactive discussion that focused on how we, as information communications technology professionals, deal with security in our various roles. *[Editor's note: If you missed this event, you can purchase eight sessions from this seminar that are video-streamed on the ACUTA website.]*

During the session it occurred to me that because our various roles are so spread across the IT spectrum, it's hard to focus on how we, as a group, should best deal with security. Something else that occurred to me was that while most of our job is very focused on using cutting-edge technologies, we too often view security from the broadest of spectrums and try to effect change using tools and processes from years before to fight cutting-edge technology threats.

Whether in the network operations center, in network infrastructure, as a systems admin, in telecom, in student services, or in the security office, we all have a different slice of the security spectrum. The problem is that security isn't the same for each of us. Information security,

cybersecurity, network security, and user education are all pieces of the pie. I won't try and lecture anyone on the best way to apply security in his or her own areas of expertise. Each of the professionals I have come to know in ACUTA is very good at what he or she does. Your involvement in this organization shows your commitment to stretching your knowledge, networks, and experiences. This allows you to make better contributions to your job, your department, and your school. What I would ask each of you to do is think beyond accepted processes and protocols. If you don't have a relationship with the information security office (ISO), take one of their analysts to lunch to hear their perspectives—you might be surprised at what you'll learn.

### Effecting Change

Too often we try to protect our customers from themselves by influencing their behavior. Don't click through! Don't open that e-mail! Don't leave your computer unlocked! Don't go to that website! And the list goes on. I'm not sure how effective we have been or continue to be. I was talking to David Ulevitch, former Washington University in St. Louis ResTech student tech and current CEO/founder of OpenDNS, who told me, "Changing user-driven behavior is hard." His entire business is built around the idea that technology should be able to provide "automated protection against advanced attacks for any device, anywhere" (www.opendns.com). Our ISO security analysts agree. They believe we shouldn't count on customers for any amount of IT security protection. Security professionals have come to believe that security has to be "baked" into technology systems from the ground up. It doesn't work nearly as well to try to add it after the fact.

One thing I do believe from talking to other security professionals is that we, as an enterprise IT community, can make a difference to our user community by trying to focus on simple, individual ways to change mindsets. Great leaders understand that giving clear, clean guidance and objectives is the best way to effect positive change. Change is hard, and changing behavior is harder yet. We all know that most people simply write down the passwords we force them to change every six months. We know most people simply walk away from their computers to take breaks. We know that most people don't change the account/passwords on their home routers. And I maintain that most people are probably okay.

My computers and devices with the Windows operating systems are set to get regular patches and updates, the firewall security is on, and I tend to use Firefox as my primary browser. I do help my son whenever he gets a new computer to have those things set up. Other than that, I try to give him simple, clear thoughts every once in a while to try to change his mindset.

One of those thoughts is that no reputable service will EVER randomly ask you for your personal information in an e-mail or ask you to click a link to enter those things. We try very hard to convey this idea to our students, freshmen especially—that the university will NEVER randomly ask them for account names, passwords, or personal information. They should ALWAYS reach out to whomever they think is originating the request to find out.

Another simple, sound, mindset change to impress upon your students, staff, and faculty (primarily staff and faculty) is that sensitive data is just that—sensitive! Storing, transferring, e-mailing, and sharing this sensitive data outside of normally accepted standards is not a good idea. One of my primary concerns a few years ago, when I ran the campus network, was that some departments were running "shadow" HR systems—data downloaded on a regular basis onto local systems that allow for easier access for a particular department or function. These are not a good thing, I think we would all agree. One of my other favorites was storing data backups on thumb drives. Another non-good thing to do.

One way to change those mindsets is not only through better audit processes, but also through steady, clear messaging. We're all keenly aware of security breaches that seem to happen even on the best of campuses, and no one wants to be responsible for exposing PII—personally identifiable information. You may not take a hit, but then again, you might. And a direct hit can cause damage in multiple directions.

Don't get too hung up trying to be too much security to too many folks on your campus—unless that's your job. Focus on the mindset changes that might best apply to your space and then talk to your security team to get their feedback. They (your security team) like to get free lunches, so take advantage!

### By the way ...

Besides doing those other security steps for my son's laptop, I also worry about his other devices. I've heard about a company that provides a cloud-based network security service that delivers automated protection against advanced attacks for any device, anywhere. They have corresponding services for business clients as well. For my son (and for me to some extent), I know that this service will protect all his devices, and it only costs me a small annual service fee that I'm happy to pay. Hey wait, did he change my mindset and I didn't realize it? Hmm. Whaddya know ...

*Matt Arthur is director of incident communications and media services at Washington University in St. Louis. He is a former president of ACUTA and currently serves on ACUTA's Ambassadors Task Force and the Journal Editorial Review Board. Reach Matt at arthur@wustl.edu.*

•

# Holes in University BYOD Policies

## Colleges rely mainly on traditional network access controls rather than new policies and systems to ensure data safety on mobile systems

*by Paul Korzeniowski*

Increasingly, faculty, staff, and students use a variety of mobile devices (smartphones and tablets) for pleasure as well as work. As a result, universities need to strike a balance between meeting individuals' desire to use these systems and protecting sensitive information. In the past few years, many businesses have been crafting new policies specifically designed to address mobile data concerns. In fact, an Osterman Research survey found that four out of five companies have or were developing BYOD (bring your own device) policies.

Universities seem to be traveling down a different path. "We do not have a policy specifically for mobile devices," said Tom Branam, telecom manager at Utah Valley University, which has 38,000 students and 1,500 employees. Instead of a mobile policy, schools are simply extending their existing equipment usage policies to handheld systems. In many cases, they do not have the interest, the time, or the funds needed to implement BYOD policies.

Extending existing policies does provide a few security checks. Theoretically, unauthorized users would not be able to access academic networks. However, many universities are not equipped to handle the special problems that mobile devices bring. For instance, they are unable to track whether confidential information is making its way onto portable systems and potentially to other places. They are unable to wipe the device clean if it is lost or stolen. These schools may be at risk for mobile data breaches.

### Back to the Stone Age

Since the days of the mainframe, schools have had IT usage policies, and those policies were extended as first PCs and later laptops became key ways for employees to complete their work. In many cases, schools are adding mobile systems to the mix. "Mobile device types change so rapidly that we have relied on a policy that focuses on the appropriate use of campus computers and IT systems," said Andrew Nichols, unified communications service manager at the University of Illinois at Urbana-Champaign (UIUC), which has 44,500 students, 2,500 faculty, and 4,100 employees. "By creating policy about the appropriate use of campus IT resources, we can rely on one set of rules for all devices," Nichols says.

A usage agreement typically includes basics for keeping the system safe and its software up-to-date. The user agrees to maintain the original device operating system and keep the OS current with security patches and updates, as released by the manufacturer. In addition, the individual sometimes installs and maintains the antivirus (AV) protection on the devices although the AV software in use is typically chosen by IT.

In return for these duties, the person is then granted access to academic system computing resources. Currently, schools rely on various system and network authentication mechanisms to ensure that information is protected and only the right folks access these resources. For instance, one university (which asked to remain anonymous) has approximately 11,000 students and 2,000 faculty members and employees, and it verifies identities by 802.1X authentication, RADIUS servers, and Microsoft Corporation's Active Directory, according to their security analyst. The system is set up to provide Web access only to students and full access to academic systems to employees and faculty members.

### Relying on Encryption

When tinkering with information, schools want to ensure that device-level encryption is used, so interlopers cannot sit on a connection and intercept information. Consequently, some schools require that individuals use a virtual private network (VPN) link when connecting to school resources. "Anyone who accesses the network off-site has to come in via a VPN," said Keith Fowlkes, CIO at Centre College, which has 1,400 students and 350 employees.

Universities typically require that the person create a user ID and associated password. In some cases, they may require multifactor authentication—something in addition to a password, such as a token—before letting the individual work with an application. These basics have been in place for decades and have done a good job of protecting sensitive information for most systems.

However, when mobile systems are involved, the technology/user relationship and ensuring data security become more complicated and prone to more potential problems. First, colleges can implement mobile programs in many

ways. If a school issues the system to the person, it usually has tight control over the system as well as its use. Typically, individuals do not have a right, nor should they have an expectation, of privacy while using school-provided devices. Universities have access to information whenever the person uses the Internet, e-mail, and voice communications. By accepting school-provided devices, individuals consent to others monitoring the device, including the contents of any files or information maintained or passed through the system. To the extent that users doubt that their private activities remain private, they need to avoid using the school-provided device for personal use.

### Dividing Lines Get Murky

Guidelines quickly become murkier when the employee or the student works with his or her own system. The college's goal is to protect sensitive information, such as grades, health information, personal data, or school financial data, while enabling the person to work with a familiar system. However, what constitutes sensitive information is subjective and often difficult to determine.

First, the school needs to evaluate various data types and determine if any should be off limits. The process can be time consuming, tedious, and open to interpretation. For instance, a college could define sensitive content as e-mail and business-related documents but exclude photographs, the assumption being that photos would be personal in nature. However, staff may take photographs of white boards containing school information. It isn't safe to make assumptions about what is business and what is personal based solely on data types.

Application type is another nebulous boundary. Third-party mobile applications have become quite popular. In addition to enabling financial personnel to access the accounts payable system, they also let individuals play video games and listen to music. Users typically are allowed to download third-party applications on their mobile devices. One problem is hackers have infiltrated many of the mobile application stores (the Android store is notorious in this area) and spawned a variety of bogus programs. So separating the good applications from malware is difficult at best.

### Taking Sensitive Data in Users' Hands

Theoretically, schools could try to stop users from downloading any data onto their personal devices, but that goal is often difficult (many would say impossible) to attain. A variety of workarounds have emerged, enabling individuals to bypass security checkpoints. The user can "jail break" the device by installing software that allows the user to bypass standard built-in security features and controls.

Typically, schools ask that individuals do not download and transfer sensitive data to other systems, such as a USB drive or a consumer cloud service. Also, the user often agrees to delete any sensitive files that may be inadvertently downloaded and stored on the device. But making sure such policies are followed is impossible. Sometimes, users do not read the agreement. "I don't have any metrics to support this, but I suspect the policy on appropriate use of computing resources is not widely read," stated Nichols at UIUC. Another challenge is that the device is often shared with other individuals or family members. A teenager will be more capricious in the use of the system than a parent.

So security mechanisms must be put in place to safeguard confidential data stored on personal devices. One approach to protecting the data is containerization, which segments the user information and school information on the device. An outsider may access the person's data but would need a password or security token to access the sensitive information.

### The Expectation of Privacy

Some universities support the systems; others let the users fend for themselves. In both cases, the school needs to clarify when communication department technicians can access the device and what they can do with it. Here again, a delicate balance needs to be struck.

The techie may be responding to legitimate discovery requests arising out of administrative, civil, or criminal proceedings, but schools need to ensure some measure of privacy. The techie cannot rifle through personal communications, such as contacts, apps, data, or pictures. Universities cannot invoke rigid policies such as "blacklisting" sites and blocking apps on the device. The school cannot use location tracking to track the person's movements.

If the device is lost or stolen, requirements change. The goal for the user and the school is to find or disable the device ASAP. First, the user needs to notify the college as soon as practical after the device has gone missing. Ideally, the school would lock the system, disable it, and perhaps start wiping out information, such as e-mail messages. If it does wipe data, the university has to ensure that personal content is not deleted without the individual's permission. The user's desire to keep the data must be balanced with the school's intention to keep the information safe.

### Keep It Simple Stupid

Even though the challenges have become quite complex, universities need to keep their policies as simple as possible. They are not generally large policy documents. On the low end, they may be a page or two. In other cases, they can be the size of a small booklet, with dozens of pages. The policy is of no use if it is not read. So, with any BYOD policy, the users have to acknowledge that they reviewed the policy. In businesses, there is a separate document. At universities, students and staff have to adhere to the university handbook, which outlines the school's policies and procedures, so IT equipment usage guidelines are often included there.

What happens if the user does not abide by the terms? In many cases, nothing. In addition to outlining the policy, a college needs to put monitoring mechanisms in place to check for compliance to university requirements. Outside of initial network access, most colleges lack the tools and personnel to ensure that users keep confidential information safe.

Mobile device management (MDM) systems deliver real-time monitoring of system usage and data access. The system can generate alerts to both the user and the IT administrator if any security policy violations occur. The tools generate audit reports that help schools contain and address risks associated with BYOD. Analytic functions correlate usage patterns and logs relating to enterprise data access and business-related communications to reveal threats and potential security breaches, which can then be addressed.

Yet, few schools have deployed such systems. "The issues with MDMs are finding the funding and people to run the system," explained the security analyst in information systems at a mid-size university in Kentucky. Many schools lack the support from college executives to deploy and run such a system. Even today, some university presidents do not fully understand security risks and therefore are unwilling to provide the needed funding.

Finally, academia is a place of few restrictions. Universities like to promote open systems (and the open exchange of ideas) and tend to balk at putting monitoring functions in place.

### How Much Risk?

So, how much of a risk are schools taking? That is the million-dollar question that no one can truly answer. Theoretically, individuals now access only select information. However, communications departments lack the tools and personnel to verify that assumption. Consequently, the possibility exists that someone may download confidential information that could fall into nefarious hands. Current academic mobile policies are a start, but they have holes that will remain until universities can invest more to secure information used on mobile systems.

*Paul Korzeniowski is a freelance writer who specializes in communications issues and is based in Sudbury, Massachusetts. He has been writing about these issues for more than two decades and can be reached at paulkorzen@aol.com.*

•

# The Impact of the Smartphone Ecosystem

## Interaction will be the key to the second half of the decade

*by James S. Cross, PhD*
*Contributing Editor*

As the PC era wanes, the smartphone ecosystem offers a new paradigm for content access and app development at colleges and universities. The paradigm shift is huge in scope, with the potential to impact the entire higher-education technology ecosystem. It offers the opportunity to leverage and get the best of all options in provisioning campus access, as it offers a cheaper technology innovation model.

The smartphone ecosystem has changed and reshaped world cultures in a very short time. The capability to provide granularity with data analytic tools in accessing massive amounts of information makes all kinds of things possible. Each successive wave of smartphone technology has injected a new dose of optimism about the future. Everywhere we look, there is a specialized app for accessing live events, uncovering hidden trends, and amassing useful knowledge nuggets.

The smartphone app revolution may not even have peaked, as many experts expected a plethora of new devices and product enhancements to be announced at the January 2015 International Consumer Electronic's Show. According to their 2014 report, Ericsson's ConsumerLab's 10 Hot Consumer Trends, 2015 promises greater globalization, increased streaming, gesture-driven smart watches, thought-controlled TV remotes, e-wallets, and stronger, more secure encryption.

Colleges and universities, as well as private industry and government agencies, must be primed to digest, assimilate, and accommodate a wide range of new possibilities as the U.S. economy continues its upward climb in 2015.

### Key Issues and Concerns

Gartner analysts indicate that as we enter 2015, global smartphone sales will account for over 50 percent of overall mobile phone sales—with the top three smartphone operating systems with Android, Apple, and Microsoft dominating the marketplace. The ability of companies to innovate rapidly has allowed the industry to repeatedly reinvent itself and evolve from bulky to sleek designed products and consumer services.

One way to understand the smartphone ecosystem is to think about your daily life. The smartphone has opened the door to new possibilities of sequencing and validating actions and behavior. Digital character is the user footprint left behind in the world of smartphones. The trend is fueling an intense revolution in data filtering to get a bird's-eye view in validating user behavior. With your smartphone, you send a text message, pass a security camera, call your boss on your way to work, buy breakfast at the local diner, take a parking ticket, and pass through company security on the first floor. Taken alone, this is disjointed information, but taken together it is your digital character for the first two hours of your work day.

In addition to rapid growth, the industry faces a number of challenges, regulations, checkpoints, key issues, and concerns related to privacy and security. Consider the following list:

- Content and data explosion
- Content filtering and granularity
- Content prioritization
- Content binge consumption
- Bandwidth shaping
- Global-footprint coverage
- Costly regulation
- Technology innovation
- Virtual currencies
- Network migration
- Multiple smartphone hardware and software platforms
- Multiple system development kits
- Campus apps portfolio management
- Customized apps development standards and code certification
- Antivirus and security software

***Everywhere we look, there is a specialized app for accessing live events, uncovering hidden trends, and amassing useful knowledge nuggets.***

The dark side is that mobile malware has intensified with the proliferation of smartphone era technologies. The growing popularity of smartphones, with all they can do, has brought an increase in viruses, malware, spyware, phishing, and other predatory entities targeting smartphone hardware and software platforms. Proactive protection is vital to safeguard

In a number of Ericsson ConsumerLab studies, we have seen that consumers do not mind sharing personal information when they believe they are getting something of value in return. However, giving away personal information without consent and for no obvious reason is something that is disliked by most people.

For this reason, there are areas where people would prefer to keep their information to themselves and not have to divulge personal details in order to complete everyday tasks. Paying with cash does not automatically lead to the dissemination of personal information and, therefore, avoids exposure to subsequent unwanted advertising or spamming from the seller. Forty-seven percent of smartphone owners would like to be able to pay electronically in a similar way—without an automatic and unavoidable transfer of personal information.

Another area where consumers feel entitled to their own privacy is personal communication, including: 56 percent of smartphone owners would like all email, chat and other internet communication to be encrypted. Over half agree that using fingerprints would be better than passwords for this.

*Source: www.ericsson.com/res/docs/2014/consumerlab/ericsson-consumerlab-10-hot-consumer-trends-2015.pdf*

smartphone devices from every angle and form of malware.

### Fueling the Next-Generation Network

The smartphone ecosystem has empowered people and changed the way most of us live, work, and play, in spite of the inherent risks. With advances in technologies, organizations and people are now able to interact globally and develop behavior patterns once considered impossible. These advances have allowed societies to analyze the world from many different perspectives, dimensions, angles, and outcomes as we visualize the possibilities of the future. With a broad range of analytical capabilities, organizations are now able to explore all aspects of an event or business opportunity and think, connect, share insights, speculate, and make smarter decisions to maximize value.

### Summary

The smartphone ecosystem is driven by the willingness to take on challenges that once appeared to be impossible. Companies, industries, colleges, and universities driven by talented people must be agile and willing to think outside the box in envisioning the future.

With society in a deleveraging environment, a number of smartphone technology trends are emerging, i.e., increased demand for content streaming, smartphone apps for security/appliance monitoring, wearable communications devices, smart city apps and services, digital purse/currency, biometric 24/7 monitoring, domestic robots, and virtualization of museums and events.

As national boundaries lose significance in the world of communications, choosing the right technology strategy is critical to success. Colleges, universities, companies, and government agencies around the world are continuing to turn to technology to:

- Identify new and emerging markets
- Build new relationships
- Overcome cultural differences
- Make sense of what the big-data troves can tell them about business dynamics
- Identify future market trends and global opportunities
- Determine the constellation of forces driving the world economies
- Determine what matters and what doesn't in launching new products and services
- Identify major areas for app development
- Create the future in an increasingly global society

### Afterthought

In the midst of the whirlwind of change, colleges and universities would do well to look to ACUTA as a reliable and trustworthy source of information. Through its publications and events, ACUTA provides higher-education IT professionals with vital information to keep them abreast of current trends, so they will be able to proactively address the innovations and challenges foist upon them by the rapid evolution of the smartphone ecosystem and other technologies. Some of the best information and most salient advice comes from ACUTA members—the professionals whose work in the trenches enables them to see the big picture as well.

*James S. Cross, PhD, is a contributing editor to the* ACUTA Journal. *A past president of ACUTA and long-time technophile, Jim is retired from Longwood University but still very involved in the field of technology. Reach Jim at jscross22@gmail.com.*

# Phishing, the Path of Least Resistance

## UMW gets creative to meet the challenges of securing the campus network

*by Nicholas Davis*

At first glance, the idea of improving IT security controls appears straightforward. Defense in depth—including enhanced authentication and authorization technologies, improved vulnerability scanning, penetration testing, and a rigorous patch-management program—are some of the usual areas on which organizations choose to focus their efforts.

However, even with ever-improving technical controls, security breaches still happen. In fact, based on the news headlines over the past year, it appears as if security incidents are increasing in number, despite the enhanced focus on enterprise systems security. How can it be that even with improving technical controls, the breaches are happening more frequently?

If you have ever looked out your office window during a heavy thunderstorm, you've probably noticed that an overwhelming deluge of water pays no attention to the gutters and conduits designed to handle only normal discharge and drainage. When the water can't flow through the conduit, it finds a new way to escape by following the path of least resistance to its destination.

The same principle holds true for hackers facing a new generation of enhanced technical security controls. For example, those who previously relied on brute force password attacks to compromise account security have been thwarted by the broad implementation of dual-factor authentication solutions. So, they look elsewhere for an unlocked door.

### The Human Factor

More and more, cyber-criminals are turning away from their technical prowess and choosing instead to focus on the human factor, which more than ever is living up to its reputation of being the weakest link in the security chain.

At the University of Wisconsin-Madison (UWM), we have long been aware of the challenges associated with strengthening the human factor when it comes to improving our overall information security stance. We have published guidelines for strong password creation and best practices for password management. Our various information-security training presentations, informational sessions, online training, and FAQs have impressed the importance of secure password management on our employees and students. Annually, we train and quiz all staff at the UWM's Division of Information Technology, and when asked questions about how to create, manage and protect their password credentials, they all respond flawlessly.

The question that remains is, Why does occasional compromise of account credentials still happen? The answer to this question is that most account compromises happen not through technical means but rather through *social engineering*, which, simply defined, is the manipulation of trust of an individual who is fooled into providing his or her log-in credentials to an attacker under false pretense.

This is a bold statement to make—to assume that we know that despite education and training, social engineering is alive and being relied on more and more.

### Putting It to a Test

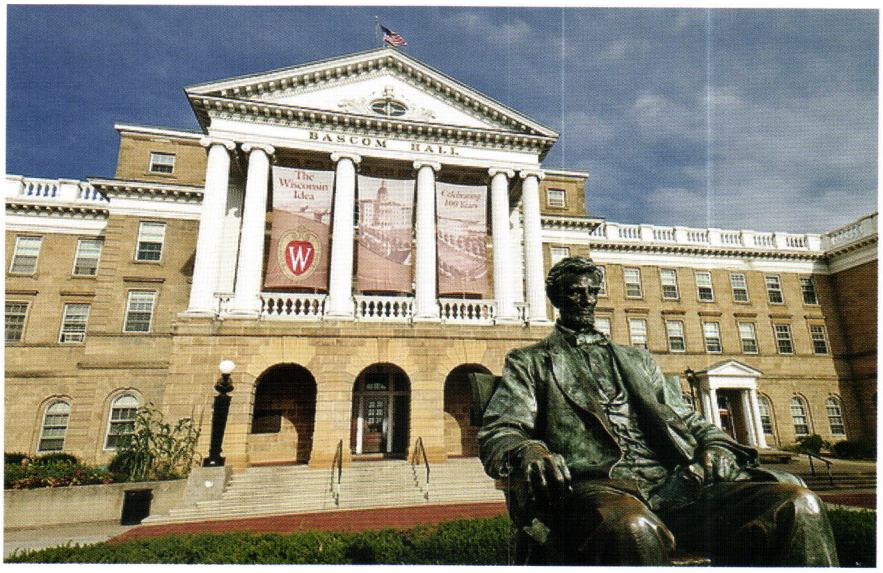
How do we know for certain that social engineering is being used effectively on our campus, even after our staff have undergone security awareness training? We know because we tested them in a real-world environment. Not just once but consistently, on a monthly basis, for over a year, via a common social engineering tactic known as *phishing*. Phishing is the act—or more appropriately the art—of baiting people with electronic communications. These communications are designed to get the recipient to click on a link, which routes him or her to a website that either masquerades as a legitimate entity, convincing the unsuspecting individual to enter sensitive information that is then harvested, or routes to a website that infects his or her computer with malware, typically a keylogger, which also harvests sensitive information.

> ***As our technical controls become stronger, the bad guys are turning more and more to exploiting the human factor as the weakest link in the IT security chain.***

When you think about phishing, thoughts of an exotic e-mail arriving from a Nigerian prince in distress may

come to mind. This type of e-mail is what our user community also perceived as phishing, and our first phishing-awareness campaign included an e-mail of similar content. The click-through rate (or politically correct term "participation rate"), was a paltry 0.2 percent, a solid indicator that our educational message of asking users not to click on message links that appear too good to be true was working well. Those who did click on the e-mail link were simply routed to a website that made them aware that they had been phished and that advised them on how to avoid falling victim to similar phishing attempts in the future.

However, what happened next provides an interesting twist to the story. After several "low and slow" phishing emails, we were satisfied that our user community knew how to recognize and deal with basic phishing e-mails.



*Bascom Hall at the University of Wisconsin Madison.*

### A Harder Test

Having congratulated ourselves on a successful real-world test, we then began to think about what to do next. After speaking with several experts in the field of social engineering, we decided to increase our level of phishing campaign sophistication by introducing two new tactics—the use of both socially and contextually aware phishing campaigns.

A socially aware campaign leverages knowledge of the recipient's familiar community surroundings, public notices, public records, and more. Contextually aware campaigns leverage an activity that the end user is likely to engage in, such as online shopping through familiar merchants.

Our first socially aware campaign leveraged a picture of Bucky Badger (the UWM mascot) embedded within an e-mail, encouraging end users to try out the "Bucky Badger Password Strength Checker" by entering their password into an online form, which would then supposedly evaluate its complexity and overall strength. Our participation rate in this campaign soared to 18 percent—that meant almost one in five recipients was willing to give away his or her password despite our educational efforts to explain to users that UWM will NEVER ask for their password in any online communication.

Our first contextually aware campaign was deliberately sent out on the day prior to Thanksgiving. It was an e-mail that appeared to come from UPS, asking the recipients to click on a link that would grant permission to UPS to deliver a work-related package a day later than planned, due to the campus closure on Thanksgiving Day. The participation rate on this campaign was 21 percent.

We also engaged in various phishing educational awareness campaigns containing UWM specific informational references, as well as logos from the Home Depot, Amazon.com, and our own registrar's office. On each occasion, we combined a subject-matter familiarity aspect (through language and logos), in conjunction with a sense of urgency to act immediately, and in some cases a threat of punishment if immediate action were not taken.

On one occasion we scattered a dozen CDs in public areas throughout our central IT building, which is home to over 500 IT staff. Each CD was labeled "Staff Organization." The CDs contained a bit of software code that was designed to report back to a central location if the Excel spreadsheet contained on the CD were opened. 25 percent of the CDs eventually found their way into end users' computers. If this had been a genuine attack, malware could have been directly installed on each end user's workstation. All the technical controls in place to filter traffic, scan e-mail at the server level, and so on are useless against malware that is introduced via local media. Workstations that don't run an effective anti-virus solution would be highly vulnerable to such an attack.

Our results indicated that our community was fully able to respond to basic phishing emails. However, we were able to eliminate users' resistance to clicking on potentially dangerous links by leveraging human nature. Specifically, the use of familiar logos and graphics, combined with information that was socially or contextually relevant to the end user or

his or her job within the university, with the usual addition of a reward (Home Depot coupon) or threat of punishment due to inaction (UPS), was critical to getting users to "participate" in our simulated phishing campaigns.

### Education Is Not Enough

From our experience, we learned that simply educating end users about general concepts of phishing is not nearly enough to protect them. Phishing often does not get the recognition it deserves in terms of the realistic threat it poses in higher education. Despite our efforts to educate, it became apparent that end users tend to forget their best practices when distracted through common social-engineering techniques.

End users suffer from a common misconception that phishing is always going to be easy to recognize. The idea that phishing e-mails typically arrive from a Nigerian prince, are written with poor grammar, and promise ridiculous sums of money should be downplayed in educational efforts. People already know how to spot this type of obvious scam. We need to focus more on the reality of the situation—that phishing e-mails, in many cases, look almost indistinguishable from a legitimate e-mail.

Our experience has demonstrated the difference between simply teaching and actually learning through experience. We found that teaching about the threat was sufficient when it came to obvious phishing e-mails, but the only way to prepare our users to deal with more realistic scenarios was to actually expose them to such threats in a controlled and safe manner.

Many organizations have been hesitant to engage in the activity of simulated phishing of their user community, based on concerns that end users may be offended that their employer appears to be trying to trick them. While this concern is valid, we do not believe it justifies avoiding the issue. While we experience occasional negative reactions from a few users who did "participate" in our simulated phishing campaigns, the benefit derived from this real-world education far outweighs the drawbacks. In fact, after several campaigns, most of the end-user community quickly began to view the phishing campaigns as an enjoyable challenge. By introducing a sense of humor into some of our phishing e-mails, we were further able to decrease end-user apprehension.

### Conclusion

Phishing and complex social-engineering techniques represent an ever-increasing threat to the information security in our academic environment. As our technical controls become stronger, the bad guys are turning more and more to exploiting the human factor as the weakest link in the IT security chain. Educating users about complex real-world, well-executed phishing through actual experience has proven to be a valuable means of helping our community better understand that we are all vulnerable to this type of attack, which more and more is coming not from a Nigerian prince but from someone impersonating Amazon.com or even our own university. Phishing e-mails such as these can really make people feel uncomfortable, as they are difficult to catch and they leverage end-user trust. However, we believe that honesty is the best policy when it comes to educating our community about the real nature of the threats they face. We plan to continue our simulated phishing campaigns and expand the service to be made available to all departments across campus in 2015.

If you are interested in learning more about the specific tools used in our phishing campaigns, how we collected metrics, and how the service is managed, please feel free to contact me

*Nick Davis is an information security architect in the division of information technology at the University of Wisconsin, Madison. He is an expert on information assurance, information technology security, cryptographic systems, security awareness, digital authentication, and authorization. Reach Nick at nicholas.davis@wisc.edu.*

As security or firewall administrators, we've got basically the same concerns [as plumbers]: the size of the pipe, the contents of the pipe, making sure the correct traffic is in the correct pipes, and keeping the pipes from splitting and leaking all over the place. Of course, like plumbers, when the pipes do leak, we're the ones responsible for cleaning up the mess, and we're the ones who come up smelling awful...

*— Marcus J. Ranum, Chief Security Officer of Tenable, a leading vulnerability management and network monitoring company*

# Institutional Excellence Award 2014

## UIUC Unified Communications Project

With the hard deadline of the expiration of a 25-year old Centrex contract as a driver, plus the approaching end-of-life dates for the campus' central e-mail and calendar systems, all faculty, staff, and graduate students at the University of Illinois at Urbana-Champaign (UIUC) were moved to a single unified-communications (UC) platform for voice, e-mail, and calendar services. Campus IT and education services (CITES), the central campus academic IT unit, initiated and executed this huge project such that the entire effort from design, planning, and final implementation took place in under two years.

*UIUC accepted the award at the Annual conference in Dallas. Left to right: Greg Gulick, Paul Hixon, Andrew Nichols, Geth Scheid, Uros Marganovic, and Tony Rimovsky, all from the UIUC; plus Jennifer Van Horn, IU, chair of the Awards Committee; and Mar'ia Adkisson, Windstream (sponsor of the award).*

The numbers demonstrate the herculean effort needed. Between September 2010 and June 2011, the e-mail accounts of over 40,000 faculty, staff, and graduate students were successfully migrated to a new campuswide Microsoft Exchange service. Between October 2011 and June 2012, over 11,000 voice lines were moved from the legacy Centrex service to Microsoft's voice service, Lync.

Besides the sheer numbers of faculty, staff, and students affected, moving them all to a converged UC system caused a substantial change in the communications culture on the campus. Taking advantage of the concept of "presence," users quickly adapted to making voice calls from their computers using Lync and began to enjoy the instant feedback provided by the chat function. Converging to one calendaring system saves countless hours when scheduling meetings. Using the audio/video conferencing function, faculty, grad students, and staff are able to attend meetings remotely that they would have missed in the past.

In addition to the new features and flexibility, departments no longer have to schedule conferences in advance or pay for conferencing. By replacing the existing campus conferencing service, a number of benefits have been realized. Departments saw an immediate cost savings and improved flexibility and functionality. CITES was able to retire the expensive solution and reclaim staff hours to focus on other projects. An unplanned benefit—and a measure of success—is that many departments that had been paying third parties for hosted conferencing solutions no longer needed these expensive services.

In order to successfully transition from many disparate systems to the one converged UC system, CITES established partnerships with the 150 IT professionals and 100 telecom (voice) unit coordinators in every major campus unit during the planning and implementation phases of the project. The degree of partnering was unprecedented, and CITES continues to build on the relationships with campus units that were established.

A successful case was made to campus administration for special one-time funding for the UC project, based on the great cost savings over the alternate solution to replace Centrex services, which required the purchase of expensive hardware and service contracts (i.e. buying a large hybrid PBX-VoIP switch).

Since all of the faculty, staff, and graduate students were affected by the transition to the converged UC system, local media (city and campus newspapers, radio stations, and television stations) ran many features on the progress of the project over time.

### Planning, Leadership, and Management Support

CITES had already been working closely with the provost's office on how to fund the projected $40 million cost to replace

the campus Centrex service. When the proposal for the conversion to Microsoft's UC system was made, the provost's office gave its support and asked the CIO to make a presentation to the campus deans to garner their support as well. The provost's office made the critical decision to loan CITES the money needed for the UC build out (while it was still operating its legacy systems in parallel) until CITES was able to start realizing the cost savings from the new UC environment.

At the onset of the project, the decision was made to make the project schedule the priority. The CITES project team was aware that this would result in uncomfortably short system testing periods before moving applications into production mode, as well as the potential for budget overruns, given the limited time to fully scope anticipated expenses. Understanding the risks of a schedule-driven project, CITES set up a multi-pronged communications plan to transparently inform the campus of the progress and problems encountered throughout the course of the project.

*The University of Illinois at Urbana-Champaign*

Given the limited time to complete the conversion, CITES used a two-prong approach to planning and implementation to cover internal and external needs. Internally, CITES hired an experienced project manager to put together the project team, create rigorous project planning and execution documents, and communicate project problems and progress. Externally, CITES worked with the provost's office to create the ATAG governance group (Academic Telecommunications Advisory Group), made up of assistant and associate deans, directors, and administrators who made IT decisions for their units. This group's purpose was to serve in an advisory role to CITES executive leadership and provide advice and review to the provost. The CIO sent out a letter to all deans, directors, and department heads and a separate letter to all campus IT staff informing them of the "dramatic communications technology changes to come" and how the "benefits of UC are worth the modest trade-offs."

Under the direction of CITES' executive director, teams of CITES staff were formed to cover every aspect of the project. This required some organizational rearrangement to leverage the various skills of staff throughout CITES, while keeping current operations running. The executive director also arranged for helpful resources to be brought in from outside CITES to supplement CITES staff. Some of the planning tasks included:

- Assessing and improving data center space in two locations to house the redundant set of Exchange and Lync servers
- Assessing the network readiness of over 300 campus buildings, which included an in-person survey of every voice and network data jack, followed by a verification of the data in CITES cabling documentation database and CAD drawings of each building
- Assessing the server and storage needs for the Exchange and Lync systems
- Working with the public safety office and the legal counsel on meeting 911 requirements with Lync VoIP
- Working with IT professionals in each unit on migration time frames for transitioning their staff first to Exchange and later to Lync
- Working with telecom unit coordinators in each campus unit on surveying the state of each existing voice land line, followed by the specifications for each Lync account to be created.
- Scheduling training sessions and materials for all campus faculty and staff

Some of the execution steps included:

- Running pilots of the Exchange and Lync systems using CITES staff, IT professionals, ATAG members, and select campus departments. Their feedback allowed CITES to assess and fix problem areas before scheduled roll-outs
- Running the conversions on days that would have the least impact on users
- Having a CITES team on site during the conversions of VIP units to ensure successful transitions
- Communicating transparently with ATAG about technical issues and potential policy issues that cropped up during the course of the conversions.
- Providing a running update of project progress on CITES UC web page and providing an FAQ for common questions.

An additional, and substantial, risk to the UC project came in the form of emergency communications. With the legacy Centrex system, each endpoint was in a fixed location. That location rarely changed. One of Lync's strongest features

is its mobility—if you have an Internet connection, you can make a phone call.

CITES was required by the campus executive director of public safety and university administration to create and demonstrate the effectiveness and accuracy of an E-911 solution for Lync prior to moving users from Centrex to Lync. The university's 911 calls are answered by a regional PSAP that handles all 911 calls in the county. The executive director of public safety included the PSAP's management very early on in the project and relied on their experience and opinion of the proposed 911 solution for Lync. In other words, the UC project would have failed without a successful E-911 solution, and the PSAP's assessment of the solution's effectiveness and reliability is what ultimately informed Public Safety's decision to allow the project to proceed. Some of the hurdles the project had to overcome included the following:

- Regional PSAP was using decades-old equipment that could only accept a 10-digit phone number rather than accepting the caller's location that Lync provides.
- Regional ALI databases take up to 72 hours to update location information, which means that real-time location information for mobile users is unavailable.
- Lync for Mac clients doesn't support location information in 911 calls.
- Routing of off-campus 911 calls to the geographically correct PSAP

The university selected a third-party vendor to provide appliances for overcoming most of these hurdles. CITES developed an excellent relationship with the PSAP and worked to address all of their concerns, complete acceptance testing, and deliver a production E-911 solution for Lync on schedule.

### Promotion of Technology and Maturity of Effort

UIUC has capitalized on the IT vision of its leaders; monetary support for IT by its chancellor, provost, and deans; and the strength of its talented technology workers throughout the campus. Starting in 2004, CITES began working on a five-year, $20 million project to upgrade the physical infrastructure for the data network in 155 buildings. With the support of the president, CITES also facilitated the creation of a private fiber ring to connect the University of Illinois campuses in Urbana, Chicago, and Springfield. These two large projects laid the groundwork for the unified communications project. The success of UC was predicated on having a fast and reliable physical network on which to run it. Having private fiber to Chicago allowed CITES to locate a redundant set of UC servers in a geographically separate location. Having fast data networks in campus buildings allowed for the deployment of the Lync VoIP technology.

In 2010, the University of Illinois' Administrative Review and Restructuring (ARR) Committee reported on how to reduce administrative costs and to redirect resources as a way to continue to promote the university's mission during an extreme economic downturn. The ARR IT Subcommittee, formed to examine expenditure on information technology (IT), had been searching for more cost-effective ways to provide IT services to the university. The subcommittee was instructed to approach this task with "a thoughtful focus on cost containment while maintaining or enhancing the level of administrative services," and it was suggested that the subcommittee consider such means as "better organization of service delivery functions, process improvements, elimination of duplicative services, better articulation of responsibilities of service units, and improving decision making." From this wordy language the mantra, "Do more, with less" was adopted—with varying levels of enthusiasm—by IT Professionals throughout campus.

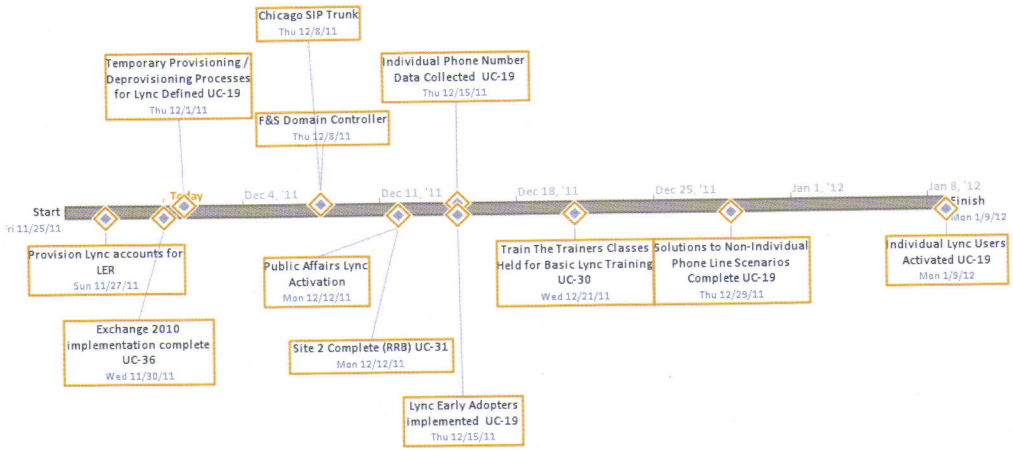
In 2010, the University of Illinois at Urbana-Champaign was in the final steps of a two-year RFP process to replace its legacy Centrex service with an expensive hybrid PBX-VoIP switch solution. With the rapidly diminishing budget climate in the state and university, high-level university committees were looking for cost-reduction opportunities in the IT realm. The executive director had just returned from an executive briefing trip at Microsoft. She was impressed by the improvements to their Exchange 2010 system with Outlook and especially by their Lync voice system, compared to the OCS voice system of that time.

Upon return, she proposed the risky but potentially very rewarding project of converting the campus to Microsoft's new UC system instead of buying the hybrid telecom switch. Though a Microsoft UC project of this size and complexity had not been implemented in any higher education environment to date, the projected cost savings and the promise of very efficient communications among faculty, staff, and students won the support of the chancellor, provost, and deans. (CITES has been happy to share its many lessons learned with other higher-education institutions contemplating a move to Microsoft's UC system.)

At the same time the UC project was launched, CITES was also working with the provost's office to implement a stable rate and funding model for central IT computing and network services. Though these were two separate efforts, choices made in one project sometimes affected the other. For example, the new rates were assessed using specific classes of FTEs. The UC project provisioned Exchange and Lync accounts for both users and "functional roles" (e.g. the speaker phone in a conference room). To convert the campus to UC, CITES arranged a campus-wide license agreement with Microsoft, which was added to the rate and funding model. With the license, departments no longer had to use their own funds to buy Microsoft products (e.g. Microsoft Office).

With enough crossover between both projects, CITES was able to use outreach

*Figure 1. Major milestones*




activities to educate UC audiences about the rate and funding project and educate rate and funding audiences about the UC project. Since both projects touched every unit on campus, CITES took advantage of every communications opportunity. Though the official UC conversion project was completed in June 2012, both the Exchange and Lync services continue to grow.

The University of Illinois has benefitted from the UC conversion project in many ways. The most obvious is that the campus community now uses a seamless platform with converged e-mail, calendaring, voice, chat, audio/video conferencing, collaboration tools, and desktop sharing. This provides new working and cost efficiencies such as easier campuswide meeting scheduling; improved remote communications for faculty, graduate students, and staff; and better collaboration capabilities both on and off campus.

Departments that used to run their own e-mail and calendaring systems have now recovered IT staff time that used to be spent checking license compliancy and supporting multiple operating systems and software versions. They also no longer have to spend money on the hardware, software, and staff to run these systems.

Some of the current IT issues the campus is grappling with are the explosive demand for support of mobile devices, new security challenges and opportunities, and developing infrastructure to create and support online and innovative learning. With a solid campus UC system in place, CITES is continuing the partnership it built with departmental IT professionals during the UC conversion to tackle these new IT challenges.

## Quality, Performance, and Productivity Measurements

At the beginning of the project, CITES created a set of UC metrics to be gathered and shared with the ATAG governance group throughout the course of the project. With such a tight time line to accomplish the conversion, the metrics were chosen to demonstrate work that was successfully completed and work that remained before the project deadline. These metrics charted the two main phases of the project—moving all campus users to the Exchange server and porting Centrex voice lines to the Lync system. Most metrics were displayed in graphical form, which made it easy to communicate progress at a glance. These were updated on a monthly basis.

It turned out to be very valuable to have this data available, since we could refer to it anytime the campus administration or the media queried us about the project's progress.

Besides the metrics charts, CITES would provide Status Reports to the ATAG, highlighting both technical and communication/outreach progress. Given the tight deadlines, discussion of any real or perceived risks was a regular feature at the ATAG meetings. Detailing them in an organized report made the discussions more focused and efficient.

## Cost, Benefit, and Risk Analysis

The budget climate at the University of Illinois in 2010 was very challenging. The aforementioned ARR Committee had released a report that included recommendations to reduce IT expenditures for the campus. CITES was looking at options to replace the end-of-life systems it had in place to provide centralized e-mail and calendar services for the campus. At the same time, CITES was about to commit to buying an expensive hybrid PBX-VoIP telephone switch to replace the university's expiring Centrex system contract. The estimated cost for the new switch was projected to be $40 million. When CITES executive director proposed using Microsoft's Unified Communications

system to replace the campus e-mail, calendar, and voice systems, running the numbers showed the potential for a return of $1.5 million dollars annual savings to the UIUC campus, starting in FY13 compared to FY10 costs.

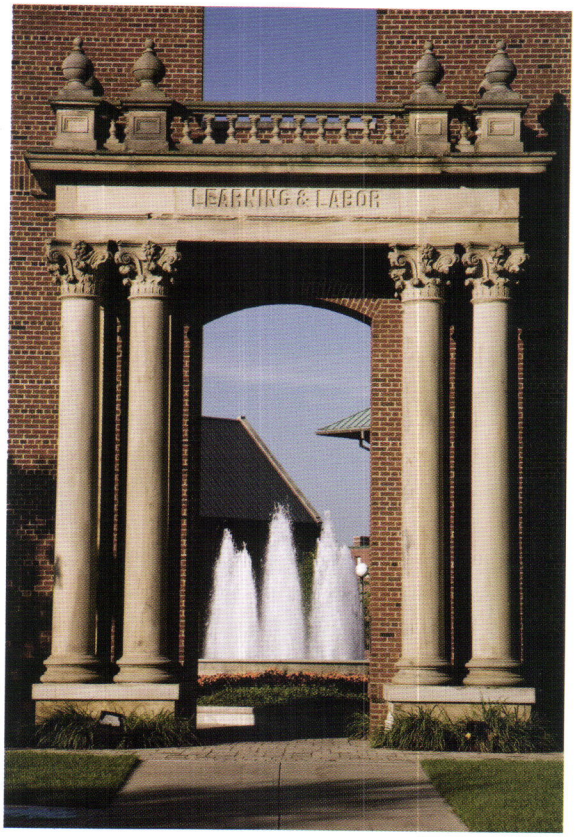
It was easy for CITES to quantify its IT cost savings for the provost's office. What was harder to do was quantify the direct and indirect IT cost savings at the department level, since few departments kept data on how much they spent on IT-related activities. The campus negotiated a very favorable license agreement with Microsoft for campus personnel with the result that departments no longer had to use their budgets to buy Microsoft products for their users, and campus faculty and staff were able to obtain Microsoft Office for personal home use at a deep discount.

At the end of the conversion, departments that had previously run their own systems realized immediate savings from the decommissioning of hardware and software needed to support departmental e-mail and calendar systems. They also realized indirect savings on IT staff resources no longer needed to support these systems.

Within CITES, IT staff that were previously needed to support the legacy campus e-mail and calendar systems were redeployed to support the new Microsoft systems. Most of CITES technicians' work shifted from installing and maintaining voice cable to installing and maintaining data cable. CITES customer service personnel who were devoted to Centrex voice support were merged into an inclusive customer service office for CITES services.

From the outset of the conversion project, campus administrators, college IT staff, and CITES staff understood the risks associated with the conversion process:

- Nothing of this scope had ever been attempted in higher education, so there were no guarantees the UC applications would perform as promised.
- Given the tight time line, CITES needed unprecedented cooperation from the administrators, IT staff, and telecom coordinators in every campus unit. This required breaking down historic proprietary boundaries.




- Faculty and staff were being asked to completely change how they used voice and data communications. This required a complete culture change from what they had been used to during their entire career at the university.
- It was not possible to carry out due diligence for all of the project-planning steps with the tight schedule. This raised the risk of scope creep and underestimating project costs.

By FY13, CITES was able to report the following numbers to the provost:

- The major campuswide UC implementation project had passed along $1,178,301 in cost savings to the campus.
- Savings on average from the FY13 Microsoft campus agreement amounted to $445K for the university.
- The copies of Microsoft Office for personal home use that were distributed in FY12 resulted in a cost savings of over $130,000, compared to the normal academic cost, and a cost savings of over $390,000 compared to the retail price.

Also, working through the ATAG governance body, the number of Exchange users was allowed to increase from the initial scope of 24,000, when ATAG agreed to add new classes of users (e.g. retirees, hourly workers, graduate students, special university affiliates.) This reduced some of the cost savings from the initial projections.

### Customer Satisfaction and Results to Date

Converting the campus to Microsoft's UC system affected every campus graduate student, faculty, and staff member. For this project to succeed, CITES had to engage and educate as many of these users as possible in the use of UC. At the start of the project, CITES had a web page in place with helpful information about what the project entailed, project status, tutorial documentation for the UC applications, sign-up and schedule information for free in-person training classes, a place to provide feedback about users' experiences with UC, and who to contact for help.

To encourage faculty and staff to learn how to use the UC applications, CITES conducted 241 UC training sessions and provided 698 annual UC training hours free to campus (with a value of $86,836 for time and materials).
CITES held a couple of UC Demo Days,

where the campus community could attend presentations with live demonstrations of "UC at Illinois" and then visit tables staffed by UC subject-matter experts to whom they could ask questions. An adjacent room was set up with a wide variety of Lync-compatible voice devices (e.g. IP phones, speaker phones, wired and wireless headsets) that the campus users could try out.

For the Exchange part of the project, CITES created outreach teams that worked directly with every major campus unit to help them successfully migrate onto the UC Exchange servers. This required a close partnership with each department's IT professionals, who were essential for moving faculty, staff, and graduate students off of privately run e-mail servers or moving them from the legacy centralized e-mail and calendar systems. CITES and the departments also had to coordinate to find a migration time that was least disruptive to their schedules.

For the Lync part of the project, CITES created outreach teams that worked directly with each department's telecommunications unit coordinators, who were essential for identifying the status of every Centrex line in their department (e.g. line still in use, voice line, fax line, alarm line) so a list could be created of lines to be transitioned to Lync. Due to the handoff constraints between the Centrex provider and the new SIP provider, legacy Centrex lines could be ported to the new Lync system on a limited number of dates. CITES worked very closely with the departments to get these port lists submitted on schedule.

CITES also partnered with a subset of IT pros and a few departments to participate in pilot trials testing the migration steps for Exchange and Lync. The feedback from these users was invaluable. It allowed CITES to report unexpected problems to Microsoft and make adjustments in its processes before proceeding with the migrations for the rest of the campus.

Besides the UC Demo Days mentioned above, CITES set up weekly "office hours" where anyone from campus could stop in to try out an array of Lync-compatible voice devices or consult CITES subject-matter experts on UC-related subjects.

A designated member of CITES' outreach team was assigned to each department on campus. Department users gave them instant feedback on what they liked and what they didn't like, what worked and what didn't work for them in their unit's migration to Exchange and Lync. This feedback was collected and shared with CITES management, the UC Project team, and the ATAG. Victories and stories of customer satisfaction were cheered. Dealing with unexpected problems and unhappy customers was a priority. Many of the users who were used to the legacy centralized e-mail and calendar systems and the land line Centrex system had a harder time adjusting to the changes UC brought about. CITES made extra efforts to train IT pros, telecomm unit coordinators, and administrative and clerical staff, so they, in turn, could be a resource for people in their units who needed help.

Given how quickly the project had to move to make the June 2012 deadline, there were a number of unanticipated problems and challenges. One of the unexpected problems involved accessibility issues. The University of Illinois' Division of Disability Resources and Educational Services (DRES) is a leader in higher education in ensuring individuals with disabilities can benefit from university programs, services, and activities, including IT services. While partnering with DRES on the migration process, CITES learned that many of the IT tools developed to help vision-impaired and hearing-impaired individuals only worked with the older versions of Outlook, which were not supported by Exchange 2010. The solution was to allow these users to remain on an older Exchange system until tools were available that worked with the newer system.

After setting the date of January 9th, 2012, for the first large campus migration to Lync and getting the relevant units prepared, our SIP provider informed us in early December that they didn't have enough temporary staging numbers needed for the mass-enable to Lync. With the holidays approaching, CITES had to fire up all of its communications channels to campus explaining the migration date would be pushed to mid-February. This had a domino effect on the subsequent planned dates for migration to Lync, and CITES had to work closely with campus units to make sure all targeted users would be migrated by the June 2012 deadline.

During the entire conversion process, at least one unplanned for issue cropped up each week. Most required small technical adjustments. The bigger ones were handled by the solid project-management process and strong internal and external communications channels CITES put in place.

One of the best outcomes from successfully converting the campus to the UC system is the trust relationships that were built between CITES and campus departments. The campus CIO has furthered this trust by creating a formal system of IT governance for CITES and campus units that is already tackling the next list of IT challenges facing the campus.

*For details, contact Beth Scheid, associate director, CITES University of Illinois, Urbana-Champaign. bscheid@illinois.edu*

•

# Advertiser's Index

★ Indicates ACUTA Corporate Affiliate

By advertising in the *ACUTA Journal,* these companies are not only promoting products and services relevant to information communications technology in higher education, they are also supporting our association. As you have opportunity, we encourage you to mention to these companies that you saw their ad in our journal and that you appreciate their support of ACUTA.



**Reach Higher Ed Clients with an ad in the *ACUTA Journal!***

For complete details contact Amy Burton, Director, Strategic Relationships

Phone: 859/721-1653 • e-mail: aburton@acuta.org

**www.acuta.org**

***Be a part of ACUTA history...***

***Write for the Journal!***

## The ACUTA Journal Wants YOUR Story!

For nearly 18 years (that's 72 issues), the *ACUTA Journal* has brought you the insights and experiences of campuses from coast to coast about every imaginable topic of relevance to higher ed technology.
We consistently hear that campus case studies are the most useful articles of all. You like to know what others are doing—what has worked and not worked—to help you make important decisions.

Has your campus implemented a new procedure or a new strategy?

Have you discovered a shortcut that might benefit others?

Is there an application or program that resolved some really tough issue for you?

The next three issues of the *Journal* fwill consider some very interesting topics:

- **Spring: Wireless Challenges in the University Setting**
- **Summer: Clouds in the Forecast**
- **Fall: Collaborating and Partnering for Success**

You are cordially invited to share your own campus story with other members via the *ACUTA Journal*. If you don't have time to write it, just **contact editor Pat Scott at pscott@acuta.org,** and she will connect you with someone who will work with you to get this done.
It's an opportunity for excellent visibility and recognition for your school, your department, and yourself.

# ASPIRE TO LEAD

ACUTA 2015
Association for College and University Technology Advancement

## ACUTA Annual Conference & Exhibition

### Atlanta, Georgia — April 19-22, 2015

DELIVER
ENGAGE
LEARN
ADVANCE

**Leaders are not born, they are forged by experience, challenges and opportunities.** Your time to lead is here as campus administrators increasingly look to you for strategies and recommendations that shape multi-million dollar investments. They look to you to solve problems when there is no manual to turn to. In fact, when you do your best work, few notice; things just – work.

From **April 19 – 22, 2015**, technology leaders will meet in **Atlanta for ACUTA's 44th Annual Conference and Exhibition**. Professionals just like you will share the latest information and their experiences, review the leading-edge technologies and services, and discuss the best ideas for confronting tomorrow's challenges. You will be writing the manuals for your own progress.

If you want to be part of shaping the future of campus technologies, if you want to meet and be inspired by your peers, if you have a vision for your campus that you want to share, then aspire to lead and come to ACUTA's Annual Conference.

TALKAPHONE

# OUR PRODUCTS HELP YOU BRAVE THE STORM.

OUR SUPPORT HELPS YOU SAVE THE DAY.


ONLY TALKAPHONE PROVIDES THE DEDICATED SUPPORT YOU NEED FOR VIRTUALLY ANY SITUATION — STANDARD.

*"(After the hurricane) all Talkaphone emergency phones were still functioning — even after being completely submerged in water and beaten hard by the debris and wind!"*

*– William Eggers, LPC, Inc.*


Download our College Security & Life Safety Communications Solutions brochure at **www.talkaphone.com/ACB4** today.

TALKAPHONE | EMERGENCY COMMUNICATION | MASS NOTIFICATION | AREA OF RESCUE

CISCO Compatible

TALKAPHONE'S VoIP-500 SERIES PHONE has tested compatible with Cisco UCM 7.1 and UCM 8.6. Go to www.cisco.com/go/compatibledisclaimer for complete disclaimer.

TALKAPHONE PROUDLY PARTNERS WITH:

exacq Technologies · comnet · milestone · OnSSI · FLUIDMESH NETWORKS · ifs · Rave MOBILE SAFETY · singlewire software